Avaya Solution & Interoperability Test Lab

Application Notes for NICE Perform® with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0

Abstract

These Application Notes describe a compliance-tested configuration consisting of NICE Perform® with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

NICE Perform® effectively provides a Selective SIP Trunk-Side audio recording solution which leverages the media replication capabilities of Avaya Aura® Session Border Controller. The solution uses CTI events from Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services to identify which media sessions are to be recorded based on a set of user definable business rules.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a compliance-tested configuration consisting of NICE Perform® with Avaya Aura® Session Border Controller, Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services.

The purpose of this integration option of Perform is to provide a scalable audio recording solution for enterprises requiring conversations with external parties be recorded for compliance or training purposes. Unlike many recording solutions, the integration with the Session Border Controller enables capture of audio calls at the network ingress/egress point when SIP trunk facilities are used. This approach has the advantage of being less taxing on communication system resources. Similar to TDM Trunk-Side recording solutions, the internal call segments between parties within the enterprise, including consultative legs of conference or transfer calls cannot be captured using the tested method. NICE offers alternative solutions for capturing internal call segments, and the combination of solutions is capable of creating a playback experience which blends recordings from multiple sources into a seamless playback experience. These other solutions were not the focus of, nor included in this compliance test.

In order for the Perform application to be able to identify which sessions to request audio streams for, the Universal Call Identifier (UCID) is extracted from CTI events obtained by monitoring internal devices (stations, ACD hunt groups and VDNs). In the tested configuration, the TSAPI service offered on Application Enablement Services was used for this purpose. All calls originating from within the enterprise have a UCID which is passed in the SIP headers from Communication Manager and Session Manager. For inbound calls, the Session Border Controller was configured with a policy to create a UCID for inbound calls that do not already have one, and to leave the UCID intact for inbound calls that do have this information passed over the public networks.

2. General Test Approach and Test Results

The compliance test focused on the interoperability between NICE Perform® and Avaya Aura® Session Border Controller. Additionally, the interface with Avaya Aura® Application Enablement Services was configured in order to enable the application to subscribe to event notification services for the internal devices. Although other elements were present such as SIP, H.323, Digital and Analog Endpoints, Avaya Aura® Communication Manager, and Avaya Aura® Session Manager, the configuration of these elements was not directly related to the interoperability of the tested solution and is not covered in detail in these notes.

2.1. Interoperability Compliance Testing

The focus of the compliance test was to confirm inbound and outbound calls could be successfully recorded. Additional test conditions were included to verify the functionality of typical call scenarios such as conference and transfer, bridged call appearances, and EC500. Serviceability testing included disconnecting Communication Manager and Application Enablement Services as well as Perform from the network, rebooting these servers as well as rebooting the Session Border Controller and Session Manager to confirm that the application was capable of recovering from typical outages.

2.2. Test Results

The objectives of the test were verified. Inbound calls both with, and without UCID being passed over the public networks were successfully recorded demonstrating the effectiveness of the UCID rules on the Session Border Controller policies. Transferred and Conferenced calls were successfully recorded throughout the life of the call with the noted exception below. For serviceability testing, the Perform solution was able to resume recording shortly after service outages.

As is expected with Trunk-Side recording solutions, internal call segments, including the temporary legs of consultative conference and transfer calls resulted in silence as these audio streams do not pass through the Session Border Controller. Calls to deskphones with EC500 activated to alert a mapped external phone (typically a cell phone) were successfully recorded whether picked up on either the desk or cell phone, as well as when handed off in both directions.

2.3. Support

Technical support for NICE Perform in the Americas can be obtained at:

- Phone: + 1 800 642 3611
- Email: support.americas@nice.com
- Web: www.nice.com/support
- Other Regions: See www.nice.com for information on contacts outside of the Americas.

3. Reference Configuration

The compliance test configuration included a Primary Site consisting of Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Aura® Application Enablement Services with several SIP, H.323 and TDM endpoints. The Primary Site used SIP trunks for signaling and call routing to and from Communication Manager and Session Manager, as well as a SIP Entity Link between Session Manager and Session Border Controller. A second site was configured with Communication Manager with SIP Trunk facilities to simulate a SIP public network service. All calls to and from the public network routed through Session Border Controller.

The NICE Perform® solution was installed on a single Windows 2003 Server including the Logger, and CLS/Interaction Center servers which are often deployed on multiple servers for scalability and other design considerations.

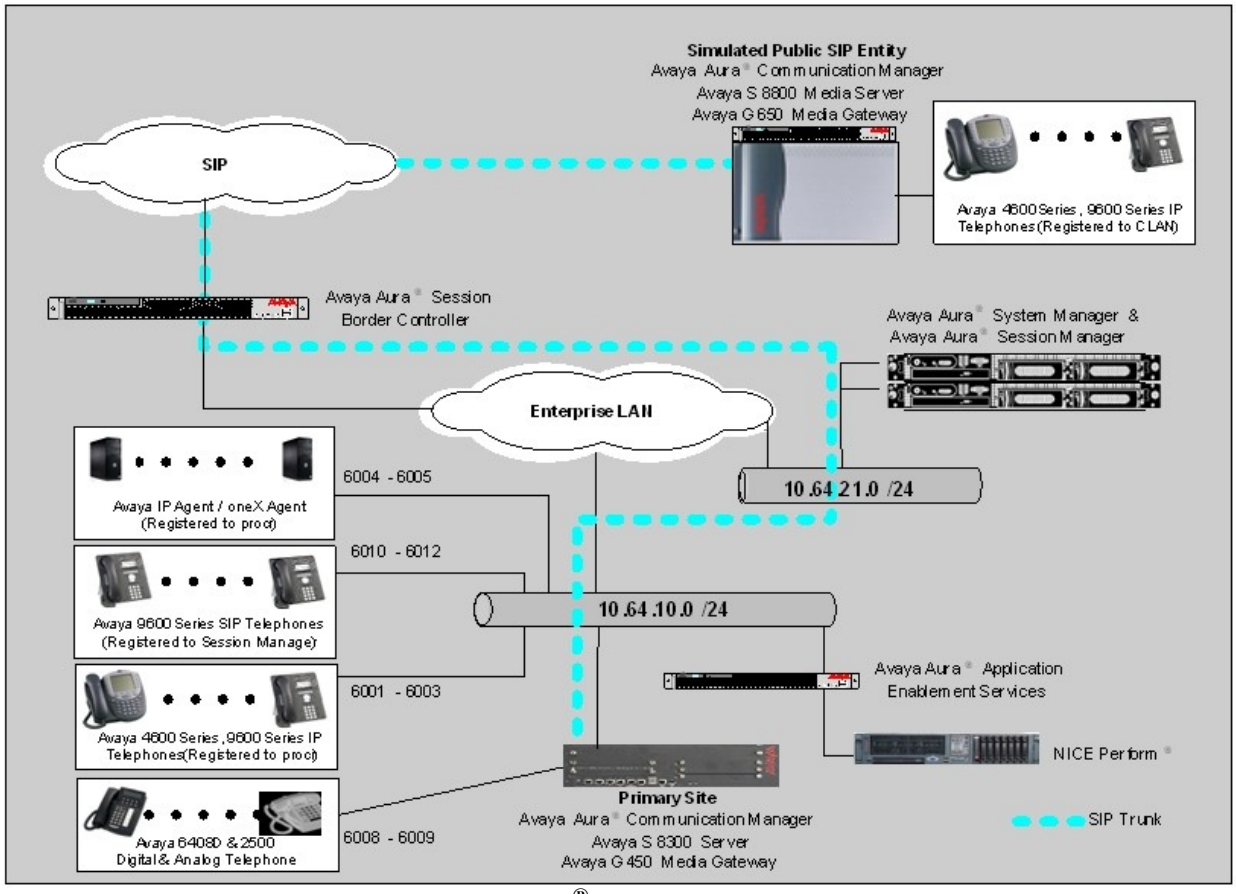


Figure 1 – NICE Perform® Compliance Test Configuration

4. Equipment and Software Validated

The following equipment and version were used for the sample configuration provided:

Equipment	Version
Avaya Aura® System Manager On Dell™ PowerEdge™ R610 Server	6.1 (Build No. - 6.1.0.4.5072-6.1.4.11) Avaya System Platform 6.0.2.1.5
Avaya Aura® Session Manager On HP ProLiant DL360 G7 Server	6.1 (Build No. - 6.1.04.0.610023)
Avaya Aura® Session Border Controller On Avaya S8800 Server	6.0.0.1.5 (E362) Avaya System Platform 6.0.1.0.5
Avaya Aura® Communication Manager On Avaya S8300D Server	6.1 (R016x.00.1.510.1 - 18621) Avaya System Platform 6.0.2.1.5
Avaya Aura® Application Enablement Services on S8500B Server	5.2.2 with Super Patch 3
Avaya G450 Media Gateway	31.11.1/1
Avaya 9600 Series SIP Phones	SIP 2.6
Avaya 9600 Series H.323 Phones	H.323 3.11
Analog Phone	-
NICE Perform® On HP DL380 G5 Server Microsoft Windows 2003R2 Server	3.2

5. Configure Avaya Aura® Communication Manager

Communication Manager used an existing configuration with SIP trunks to connect to Avaya Aura® Session Manager. Configuration of this aspect of the integration was standard and not directly relevant to the interoperability of NICE Perform®. Therefore, this aspect of the configuration will not be covered in these notes.

The steps necessary to configure Avaya Aura® Application Enablement Services interfaces to Communication Manager are described below.

5.1. Communication Manager Configuration Details

All the configuration changes in this section for Communication Manager are performed through the System Access Terminal (SAT) interface. For more information on configuring Communication Manager, refer to the Avaya product documentation, Reference **[1].**

This section provides the procedures for configuring Communication Manager. The procedures are as follows:

- Verify Feature and License are adequate for the integration
- Administer Processor Ethernet Interface for Application Enablement Services connectivity
- Administer Communication Manager System Features
- Administer Computer Telephony Integration (CTI) Link
- Confirm Station Administration
- Ensure Shared UUI is Passed Over External Trunk Facilities

The detailed administration of contact center entities, such as VDN, Skill, Split, Logical Agents and Station Extensions are assumed to be in place and are not covered in this document.

1.	**Verify Feature and License are adequate for the integration** Applications that use Application Enablement Services TSAPI must have **Computer Telephony Adjunct Links** enabled on Communication Manager. This feature entitlement is provided with each TSAPI license. TSAPI entitlements must be activated in both licenses. If this option is not set to "**y**", contact the Avaya sales team or business partner for a proper license file.

```
display system-parameters customer-options                      Page   3 of  11
                                OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y          Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                      CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                        CAS Main? n
Answer Supervision by Call Classifier? y                Change COR by FAC? n
                                ARS? y  Computer Telephony Adjunct Links? y
                ARS/AAR Partitioning? y   Cvg Of Calls Redirected Off-net? y
          ARS/AAR Dialing without FAC? n                      DCS (Basic)? y
          ASAI Link Core Capabilities? n                DCS Call Coverage? y
          ASAI Link Plus Capabilities? n               DCS with Rerouting? y
       Async. Transfer Mode (ATM) PNC? n
  Async. Transfer Mode (ATM) Trunking? n    Digital Loss Plan Modification? y
              ATM WAN Spare Processor? n                          DS1 MSP? y
                                ATMS? y            DS1 Echo Cancellation? y
                  Attendant Vectoring? y
```

2. Administer Processor Ethernet Interface for Application Enablement Services Connectivity

Enter the **change node-names ip** command. The Application Enablement Services and **procr** node-names need to be defined here.

```
change node-names ip                                    Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
aesserver2              10.64.10.21
default                 0.0.0.0
procr                   10.64.10.67
procr6                  ::
```

On most R6 servers, the Processor Ethernet Interface will already be administered in the ip-interface list. The **display ip-interface procr** command will display the parameters of the Processor Ethernet Interface.

```
display ip-interface procr                              Page   1 of   2
                                  IP INTERFACES

                  Type: PROCR
                                                  Target socket load: 4800

      Enable Interface? y                        Allow H.323 Endpoints? y
                                                  Allow H.248 Gateways? y
        Network Region: 1                          Gatekeeper Priority: 5

                                 IPV4 PARAMETERS
             Node Name: procr                  IP Address: 10.64.10.67

           Subnet Mask: /24
```

```
display ip-interface procr                              Page   2 of   2
                                  IP INTERFACES

                Speed: 100Mbps
               Duplex: Full

                                 IPV6 PARAMETERS
             Node Name: procr6
            IP Address: ::

           Subnet Mask: /64
      Enable Interface? n
```

3. **Administer Processor Ethernet Interface for Application Enablement Services Connectivity (Continued)**

Add an entry for Application Enablement Services as described below:

- Enter the **change ip-services** command.
- In the **Service Type** field, type **AESVCS**.
- In the **Enabled** field, type **y**.
- In the **Local Node** field, type the Node name **procr** for the Processor Ethernet Interface.
- In the **Local Port** field, use the default of **8765**.
- Note that in installations using CLAN connectivity, each CLAN interface would require similar configuration, Reference **[2].**

```
change ip-services                                              Page   1 of   4

                                    IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS         y       procr            8765
CDR1                   procr            0        MTS             9000
CDR2                   procr            0        RDTT            9001
```

On Page 4 of the IP Services form, enter the following values:

- In the **AE Services Server** field, type the name obtained from the Application Enablement Services server.
- In the **Password** field, type the same password to be administered on the Application Enablement Services server.
- In the **Enabled** field, type **y**.

```
change ip-services                                              Page   4 of   4
                          AE Services Administration

   Server ID    AE Services       Password          Enabled    Status
                   Server
      1:       aesserver2         *                   y        in use
```

Note that the name and password entered for the **AE Services Server** and **Password** fields must match the name and password on the Application Enablement Services server. The administered name for the Application Enablement Services server is created as part of the Application Enablement Services installation, and can be obtained from the Application Enablement Services server by typing **uname –n** at the Linux command prompt.

4. **Administer Communication Manager System Features**

Enter the **change system-parameters features** command and ensure that **Create Universal Call ID (UCID)** is enabled system wide on page 5, and that **Send UCID to ASAI** is set to "**y**" on page 13. Also, note the **UCID Network Node ID** which will be used later in **Section 8.1, Step 3**. Perform relies on UCID to identify which sessions to record.

```
change system-parameters features                              Page   5 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS

SYSTEM PRINTER PARAMETERS
  Endpoint:               Lines Per Page: 60

SYSTEM-WIDE PARAMETERS
                                    Switch Name:
           Emergency Extension Forwarding (min): 10
         Enable Inter-Gateway Alternate Routing? n
Enable Dial Plan Transparency in Survivable Mode? n
                             COR to Use for DPT: station

MALICIOUS CALL TRACE PARAMETERS
               Apply MCT Warning Tone? n   MCT Voice Recorder Trunk Group:
      Delay Sending RELease (seconds): 0
SEND ALL CALLS OPTIONS
     Send All Calls Applies to: station    Auto Inspect on Send All Calls? n
              Preserve previous AUX Work button states after deactivation? n
UNIVERSAL CALL ID
     Create Universal Call ID (UCID)? y    UCID Network Node ID: 1
```

```
change system-parameters features                              Page  13 of  19
                        FEATURE-RELATED SYSTEM PARAMETERS
 CALL CENTER MISCELLANEOUS
          Callr-info Display Timer (sec): 10
                       Clear Callr-info: next-call
       Allow Ringer-off with Auto-Answer? n

   Reporting for PC Non-Predictive Calls? n


         Interruptible Aux Notification Timer (sec): 3


  ASAI
           Copy ASAI UUI During Conference/Transfer? n
       Call Classification After Answer Supervision? n
                                  Send UCID to ASAI? y
         For ASAI Send DTMF Tone to Call Originator? y
```

5. **Administer Computer Telephony Integration (CTI) Link**

This section provides the steps required for configuring a CTI Link.

Enter the **add cti-link <link number>** command, where **<link number>** is an available CTI link number.

- In the **Extension** field, type **<station extension>**, where **<station extension>** is a valid station extension.
- In the **Type** field, type **ADJ-IP**.
- In the **Name** field, type a descriptive name.

```
add cti-link 1                                                Page   1 of   3
                                    CTI LINK
 CTI Link: 1
Extension: 6201
     Type: ADJ-IP
                                                                      COR: 1
     Name: AES-10.64.10.21
```

```
add cti-link 1                                                Page   2 of   3
                                    CTI LINK
FEATURE OPTIONS
      Event Minimization? n        Special Character for Restricted Number? n
      IC Adjunct Routing? n   Send Disconnect Event for Bridged Appearance? n
                                          Two-Digit Aux Work Reason Codes? n
                                              Block CMS Move Agent Events? n
```

```
add cti-link 1                                                Page   3 of   3
                                    CTI LINK
Bridged Appearance Origination Restriction? n

            SAC/CF Override: n
```

6. **Confirm Station Administration**

All SIP stations that will be recorded must have **Type of 3PCC Enabled** set to **Avaya** in order for Application Enablement Services to properly send all call events to the application. If this is changed while the endpoint is registered, re-register the endpoint for this setting to completely take effect. Failure to register after changing this setting could result in unpredictable CTI message issues.

```
change station 6010                                           Page   6 of
6
                                     STATION

SIP FEATURE OPTIONS
         Type of 3PCC Enabled: Avaya
                     SIP Trunk: aar
```

7. **Ensure Shared UUI is Passed Over External Trunk Facilities**

To ensure calls routed to the public network via Session Manager and Session Border Controller contain the UCID generated on Communication Manager, set the **Send UCID?** to ***y***, and **UUI Treatment** to ***shared*** on the third page on the trunk group that is used for routing calls to Session Manager. On the public side Communication Manager, these settings were identical, but the **UUI Treatment** was set to **service-provider** and **Send UCID** to **n** for some test cases to verify that the Session Border Controller would use the existing UCID, or add a UCID if none was present.

```
change trunk-group 30                                          Page   3 of  22
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                    Numbering Format: unk-pvt
                                                 UUI Treatment: shared
                                               Maximum Size of UUI Contents: 128
                                                  Replace Restricted Numbers? n
                                                 Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no
               Send UCID? y


 Show ANSWERED BY on Display? y
```

6. Configure Avaya Aura® Application Enablement Services

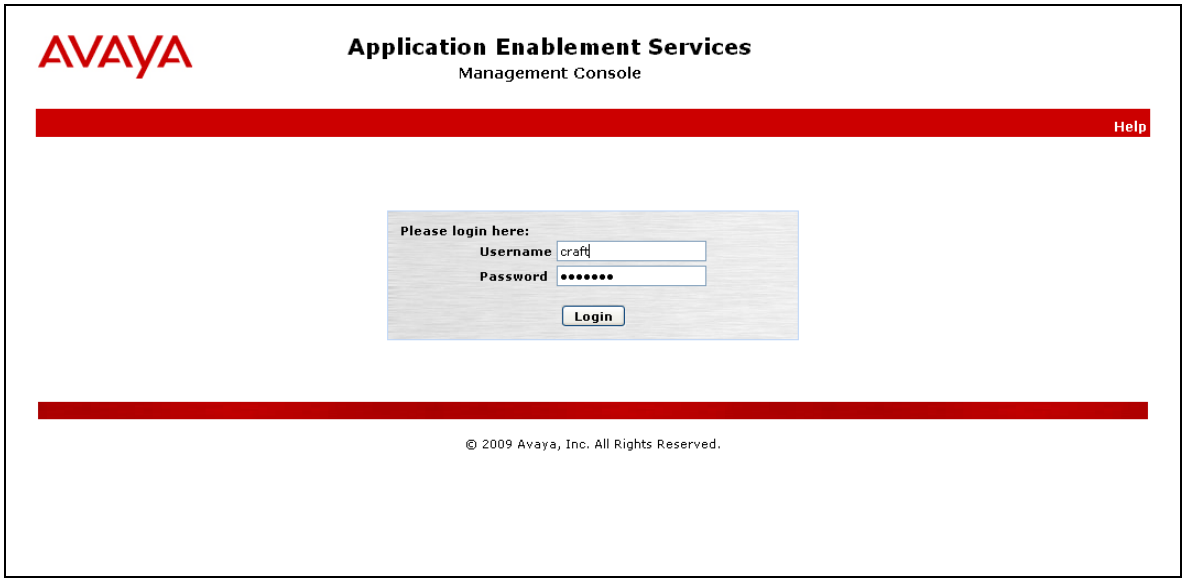
Application Enablement Services enables applications to monitor and control telephony resources on Communication Manager. Application Enablement Services receives requests from applications and forwards them to Communication Manager. Conversely, Application Enablement Services receives responses and events from Communication Manager and forwards them to the appropriate applications.

This section assumes that the installation and basic administration of Application Enablement Services has already been performed. For more information on administering Application Enablement Services, refer to the Avaya product documentation, Reference **[2]**.

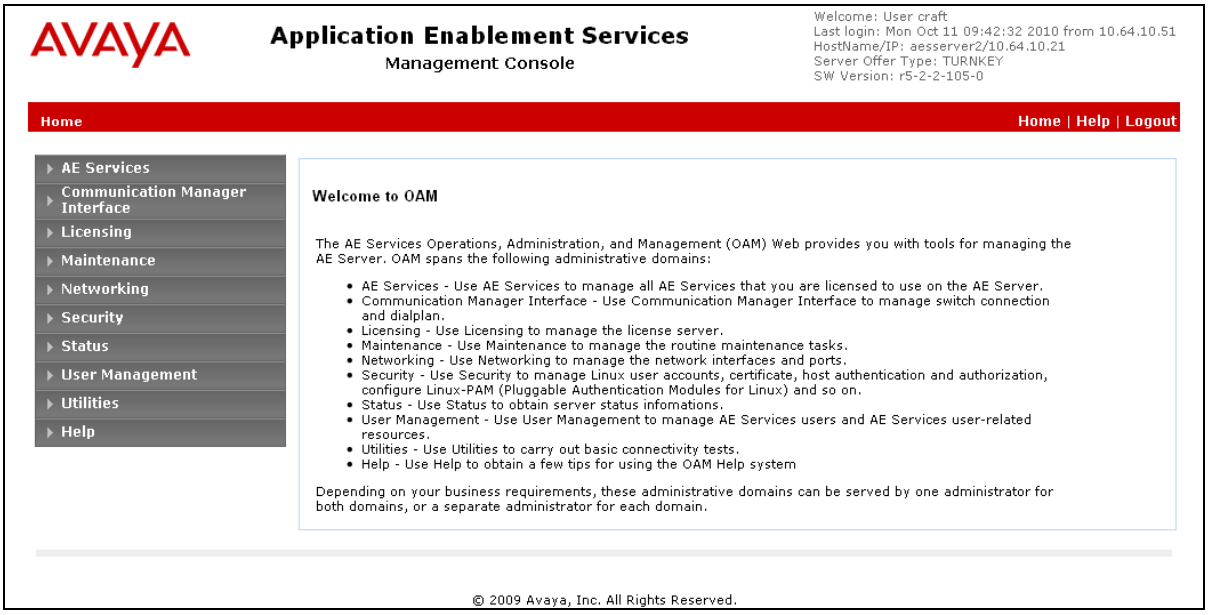
This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:

- Confirm Network Configuration
- Configure Communication Manager Switch Connections
- Verify TSAPI Licensing
- Add TSAPI Links
- Add CTI User
- Enable Unrestricted Access to the Security Database
- Note the T-Link Name

Access the web-based administration interface using **https://<ip-address>** in a browser where **<ip-address>** is the client interface address of the Application Enablement server. Click on the **Continue to Login** link. Log in using appropriate credentials.

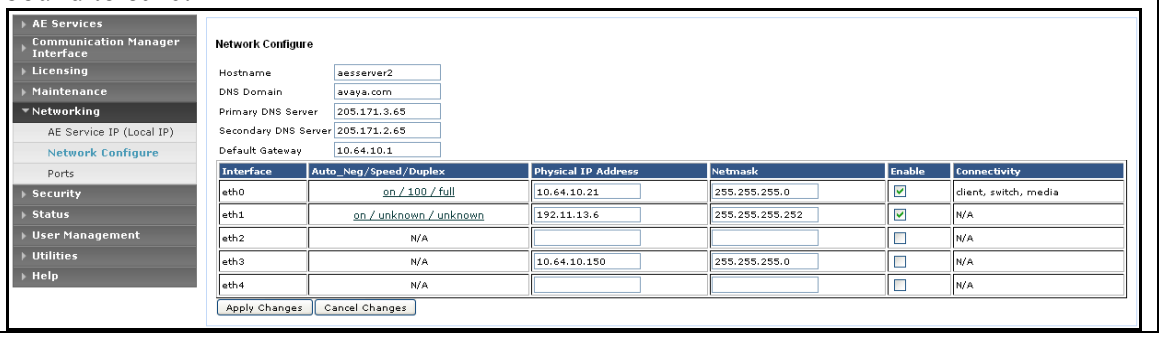


The **Welcome to OAM** screen is displayed next.



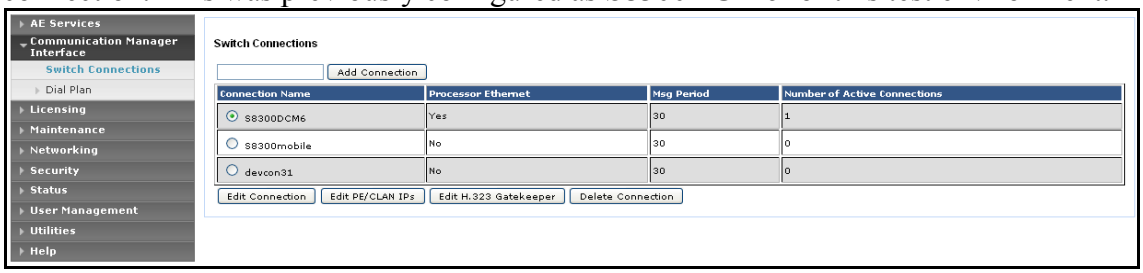
1. Confirm Network Configuration

Select **Networking > Network Configure** and note the client interface IP Address (**eth0** in this example) which will be used later in the application configuration. Application Enablement Services can be configured to use one or multiple NIC interfaces. It is preferable for security and performance reasons to use multiple interfaces and to have these on separate networks. The Communication Manager interface should always be bound to **eth0**.

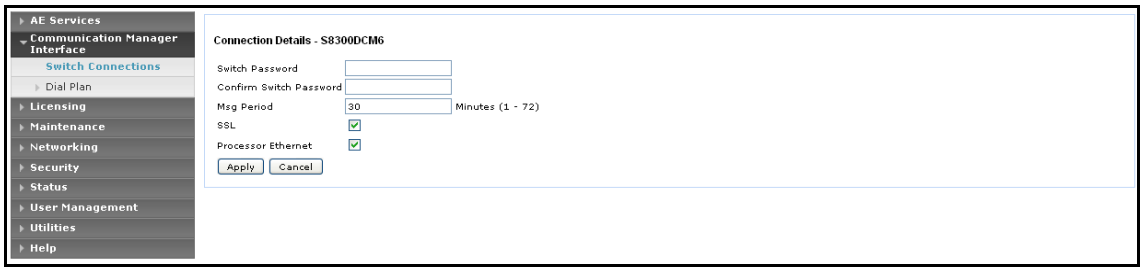


2. Configure Communication Manager Switch Connections

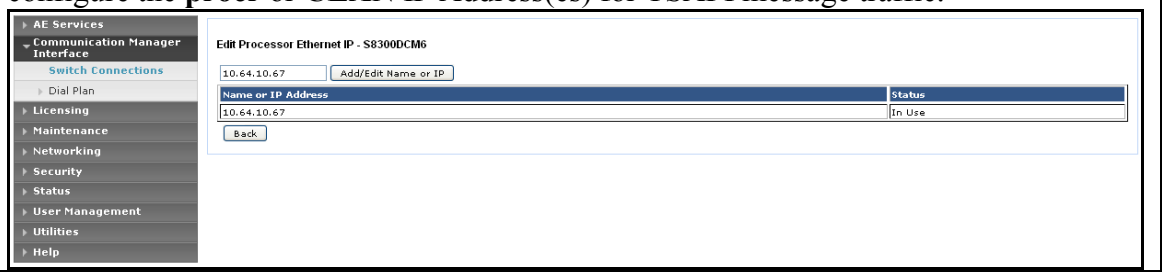
To add links for the Communication Manager, navigate to the **Communication Manager Interface > Switch Connections** page and enter a name for the new switch connection. This was previously configured as **S8300DCM6** for this test environment:



Use the **Edit Connection** button shown above to configure the **Switch Password**. This must match the password configured in **Section 5, Step.2** above. Enter the **Switch Password** and check the **Processor Ethernet** box if using the **procr** interface, as shown below.



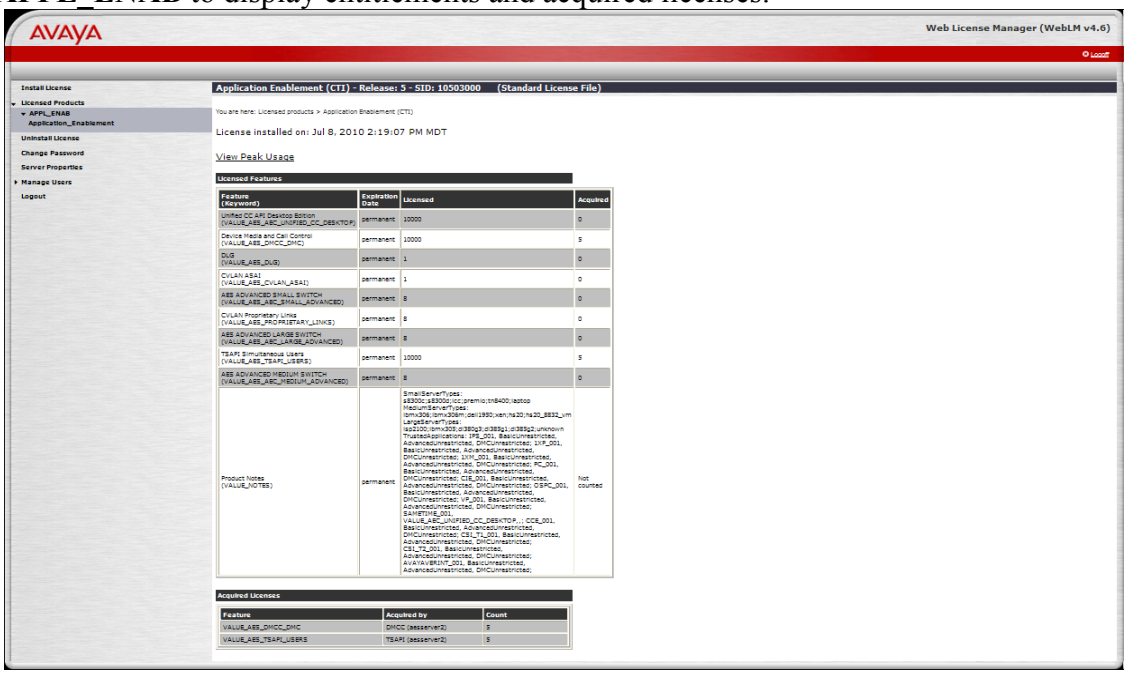
Use the **Edit PE/CLAN IPs** button (shown in this section's first screen shot above) to configure the **procr** or **CLAN** IP Address(es) for TSAPI message traffic.



3. Verify TSAPI Licensing

NICE Perform will consume a **TSAPI** license for each station and ACD Hunt Group that is to be monitored and recorded. If the number of licenses are not adequate for the integration, contact Avaya sales or an authorized reseller.

Navigate to **Licensing > WebLM Server Access** and log in using appropriate credentials. Select **Application_Enablement** under **Licensed Products > APPL_ENAB** to display entitlements and acquired licenses.



The screenshot below gives a closer look at the license counts.

Feature (Keyword)	Expiration Date	Licensed	Acquired
Unified CC API Desktop Edition (VALUE_AES_AEC_UNIFIED_CC_DESKTOP)	permanent	10000	0
Device Media and Call Control (VALUE_AES_DMCC_DMC)	permanent	10000	5
DLG (VALUE_AES_DLG)	permanent	1	0
CVLAN ASAI (VALUE_AES_CVLAN_ASAI)	permanent	1	0
AES ADVANCED SMALL SWITCH (VALUE_AES_AEC_SMALL_ADVANCED)	permanent	8	0
CVLAN Proprietary Links (VALUE_AES_PROPRIETARY_LINKS)	permanent	8	0
AES ADVANCED LARGE SWITCH (VALUE_AES_AEC_LARGE_ADVANCED)	permanent	8	0
TSAPI Simultaneous Users (VALUE_AES_TSAPI_USERS)	permanent	10000	5
AES ADVANCED MEDIUM SWITCH (VALUE_AES_AEC_MEDIUM_ADVANCED)	permanent	8	0

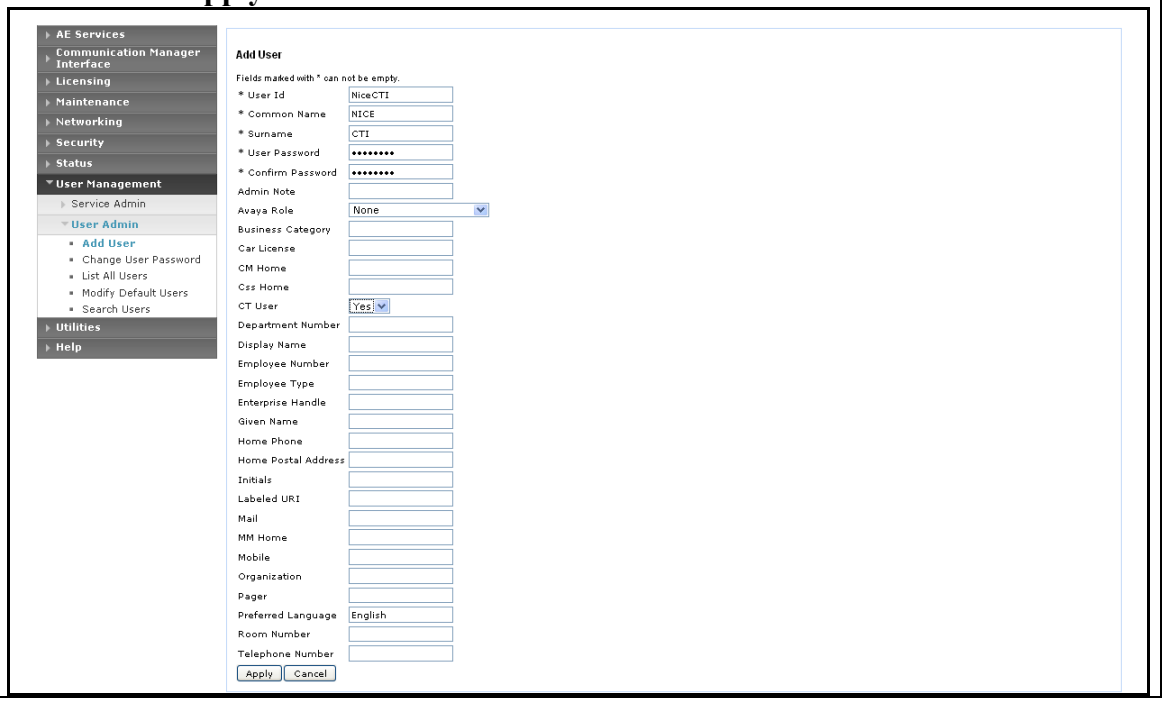
4.	**Add TSAPI Links** Navigate to the **AE Services -> TSAPI -> TSAPI Links** page to add the TSAPI CTI Link. Click **Add Link**. Select a Switch Connection using the drop down menu. Select the **Switch CTI Link Number** using the drop down menu. The CTI link number must match the number configured in the **cti-link** form in **Section 5, Step 5**. Click **Apply Changes**. If the application will use Encrypted Links, select **Encrypted** in the **Security** selection box. 

5. Add a CTI User

Perform requires a CTI user account to access Application Enablement Services. Select **User Management -> User Admin -> Add User** from the left pane.

In the **Add User** screen, enter the following values:

- In the **User Id** field, type a meaningful user id.
- In the **Common Name** field, type a descriptive name.
- In the **Surname** field, type a descriptive surname.
- In the **User Password** field, type a password for the user.
- In the **Confirm Password** field, re-enter the same password for the user.
- In the **Avaya Role** field, retain the default of **None.**
- In the **CT User** field, select **Yes** from the drop down menu.
- Click **Apply** at the bottom of the screen.

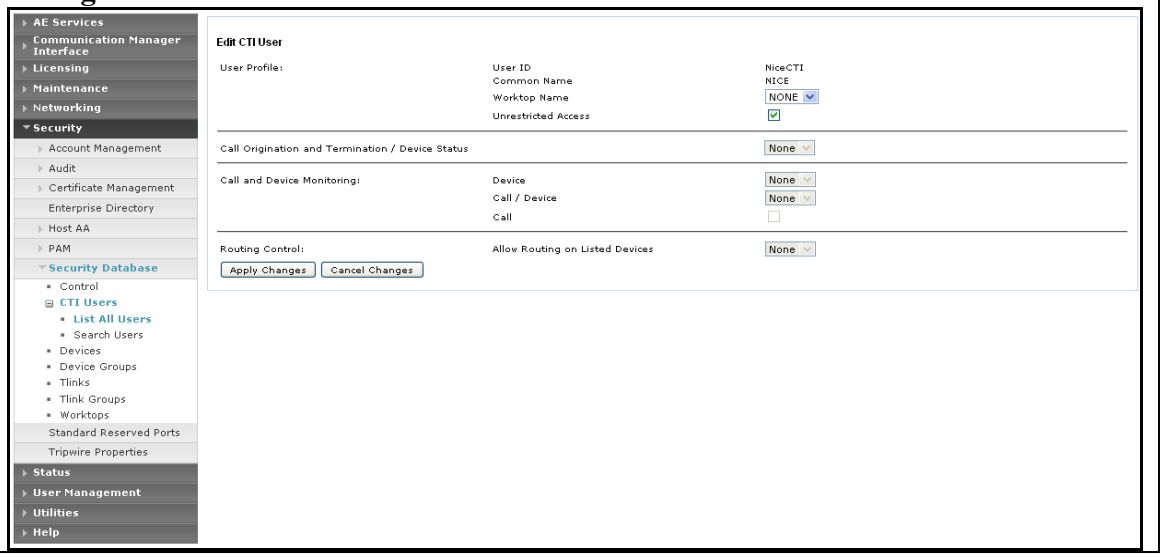


6. Enable Unrestricted Access to the Security Database

The NiceCTI user account will require unrestricted Security Database access in order to be able to access any of the Devices (stations) administered to be recorded in the application. This enables a user to administer the agent, vdn and acd devices on the Perform server and not have to duplicate the effort in the Security Database.

To change the security level for the CT User Select **Security -> Security Database -> CTI Users -> List All Users** from the left pane. Choose the CTI user, and click **Edit** (not shown below).

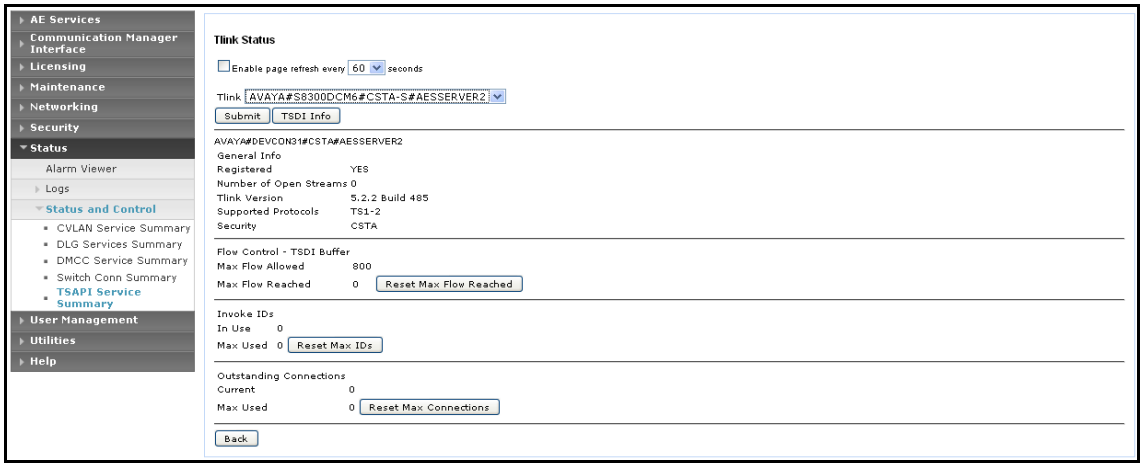
On the **Edit CTI User** page, check the **Unrestricted Access** option and click on **Apply Changes**.



7. **Note the T-Link Name**

This information will be used in the application configuration below.

Select **Status > Status and Control > TSAPI Service Summary** from the left pane and select **Edit T-Links** (not shown below). Once at the **Edit T-Links** screen, this screen shows a select box of the Tlink names. A new Tlink name is automatically generated by the Application Enablement Services server upon creation of a new switch connection. Locate and select the Tlink name associated with the relevant switch connection which would use the name of the switch connection as part of the Tlink name (not shown below). This screen will also provide information on the status of the TLink as shown below:



7. Configure Avaya Aura® Session Manager

The configuration of Session Manager followed standard configuration to establish a SIP Entity Link with Avaya Aura® Session Border Controller for receiving and routing calls from and to the public network. This configuration required nothing special for the NICE Perform® integration and is therefore not covered in this document.

8. Configure Avaya Aura® Session Border Controller

The Session Border Controller installation steps include inputs required to properly configure default Public Network and Private Network interfaces and default policies. These steps were performed prior to the testing of the NICE Perform® solution, and had no direct impact on the tested solution. The steps required to configure the interface to permit Perform to send Invites in order to be added to calls, and the associated policies needed are described below.

8.1. Session Border Controller Configuration Details

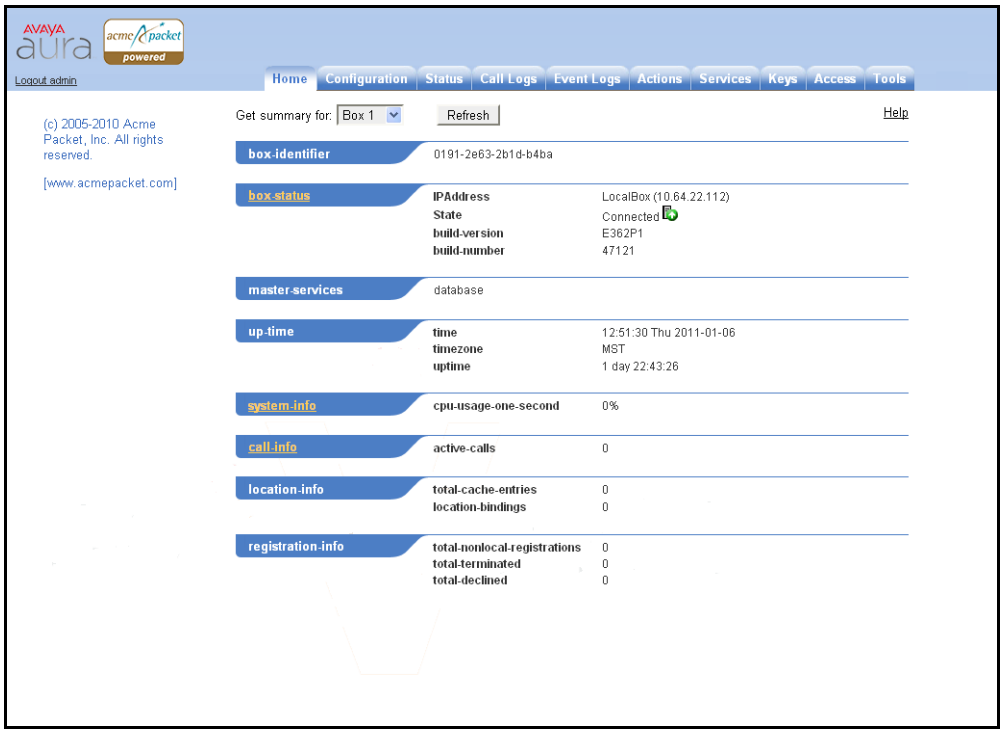
The focus of these notes is to demonstrate the specific configuration steps that pertain to enabling Perform to interact with Session Border Controller. The detailed configuration used in this test is attached in the form of a saved configuration file which can be referred to for specific details about the integration with the Telco provider (in this case, the remote Communication Manager), and Session Manager. Further, this file can be loaded into the Session Border Controller configuration to be used as a starting point for implementations at other locations.

An overview of the configuration tree follows to highlight the specific tasks necessary for the Perform integration. These include:

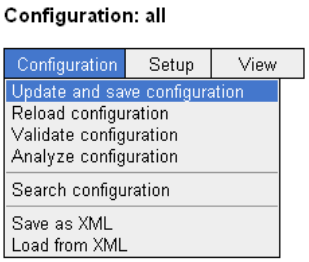
- Confirm License Capacities
- Enable Third Party Call Control for the Default Session Configuration
- Define UUI creation rules for the Default Session Configuration
- Create a Session Policy and Rule to Handle Perform Session Requests
- Create a SIP Gateway Server

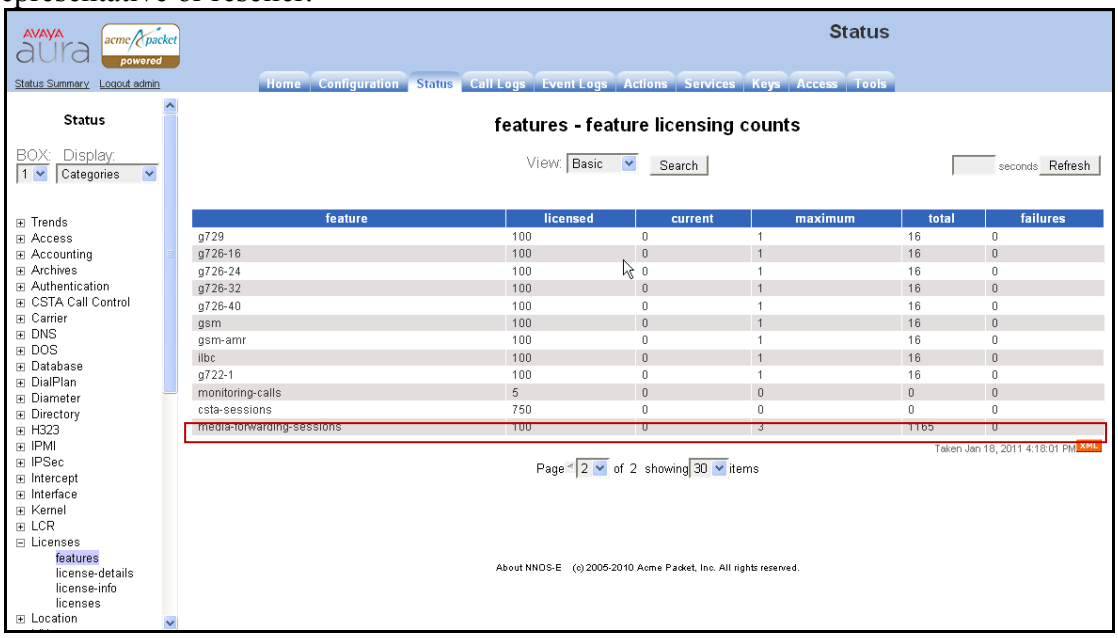
NOTE: In each case, when navigating to a setting page, it is generally necessary to enable the advanced settings view in order to configure the objects necessary for the integration. To do so, click on the Show advanced button at the top of the configuration screen. If the Show basic button is displayed, you are already in advanced mode.

Access the Session Border Controller and log in using appropriate credentials. The configuration interface can be reached via web browser by entering the URL: https://ip_address/.



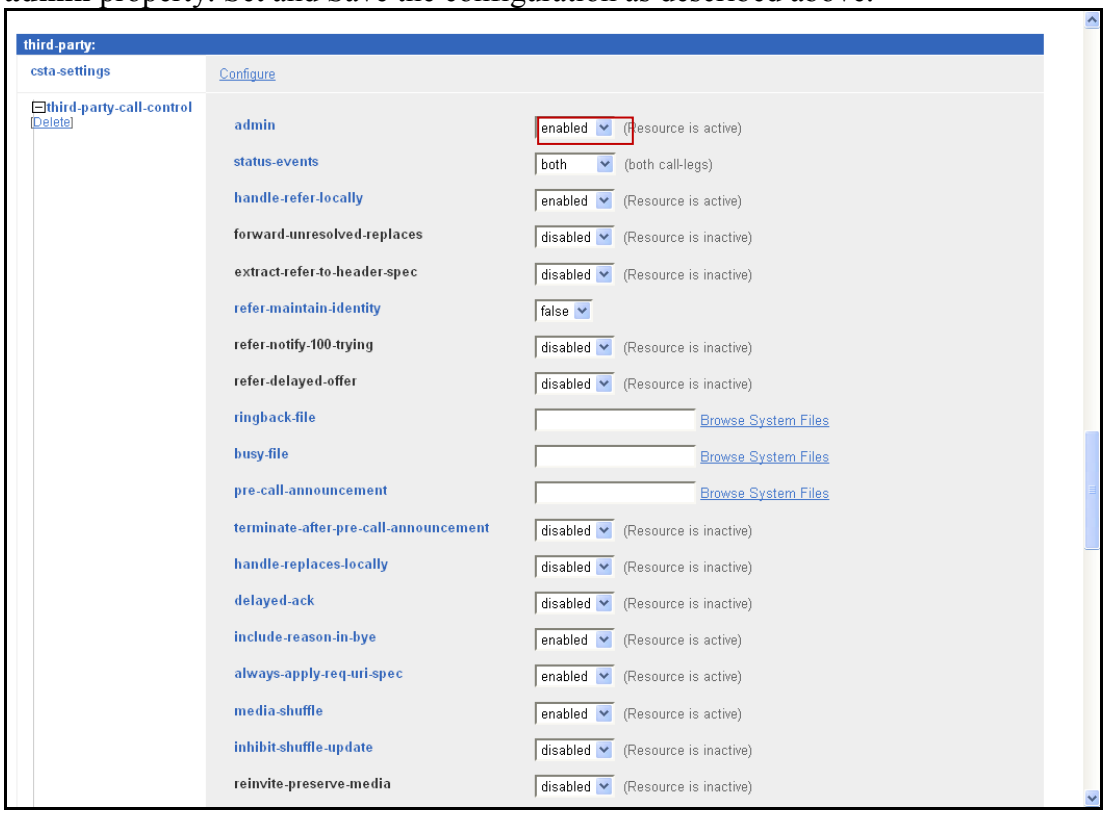
Note regarding **Set** and **Save** used throughout this document**:** After setting properties for each object, click Set which is located at the top and bottom of each page, then click on the **Update and save configuration** menu option at the top\left corner of the navigation tree. When prompted, click **yes** to both confirmation dialogs that follow.



1.	**Confirm License Capacities** Confirm that the license includes an adequate number of **media-forwarding-sessions** to accommodate the maximum number of simultaneous recordings in the configured environment. If additional license entitlements are required, contact your Avaya representative or reseller. 

2. Enable Third Party Call Control for the Default Session Configuration

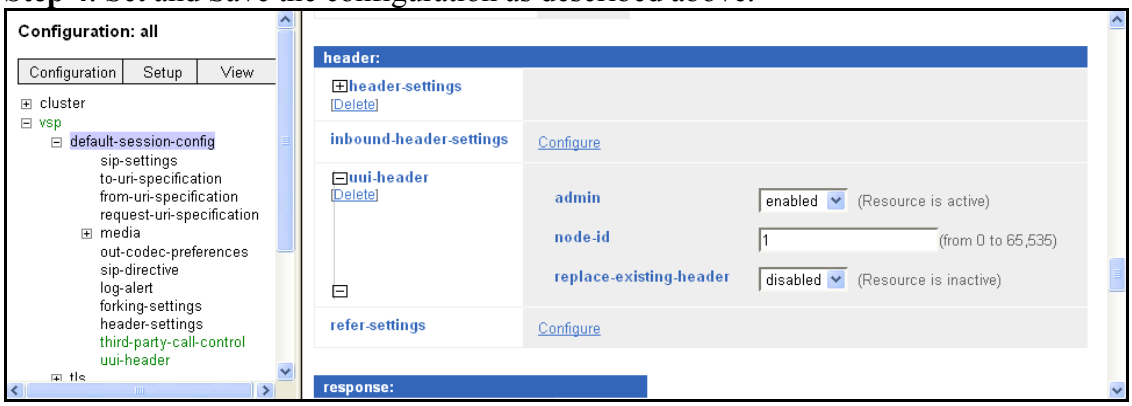
Navigate to **vsp\default-session-config** and scroll down to find the **third-party-call-control** property, click on the + icon to expand the properties. Select ***enabled*** on the **admin** property. Set and Save the configuration as described above.



3. Define UUI creation rules for the Default Session Configuration

The Perform integration requires that all sessions passing through the Session Border Controller have a UCID which will be used to identify the specific session for a given call. When calls arrive from the PBX side, they will already have a UCID in the UUI field as shared UUI treatment was set on the trunks from Communication Manager to Session Manager and/or Session Border Controller. When calls arrive from the Telco side, if the header already contains UUI containing a UCID, it will be preserved and passed on to the next hop. If a call from the Telco arrives without UCID, a UCID will be created and Communication Manager will use this UCID.

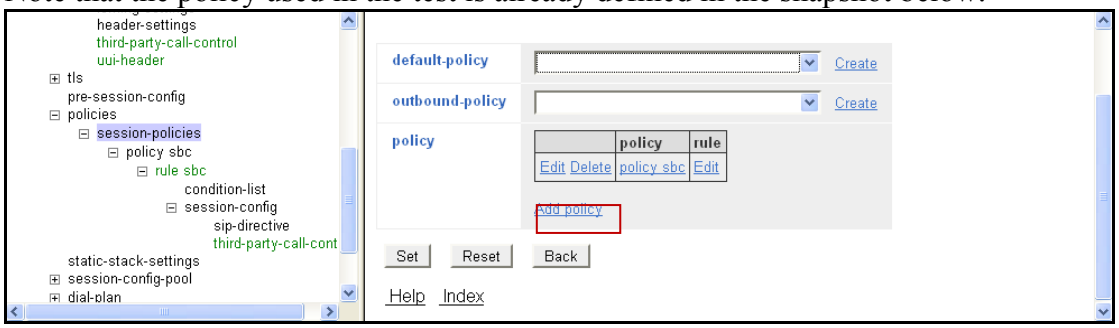
In the **header** section of the **default-session-config**, click on the + next to **uui header.** Select ***enabled*** for the **admin** property and enter a **node-id**. The node-id can be any integer value, it should match the **UCID Network Node ID** administered in **Section 5, Step 4**. Set and Save the configuration as described above.



4. Create a Session Policy and Rule to Handle Perform Session Requests

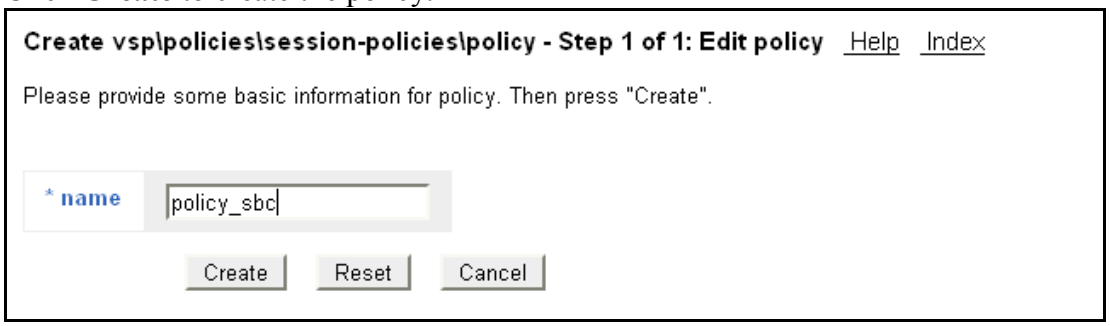
Note: This task requires several steps and spans the next four pages.

Navigate to the **policies\session-policies** property and click on the **Add policy** link. Note that the policy used in the test is already defined in the snapshot below.

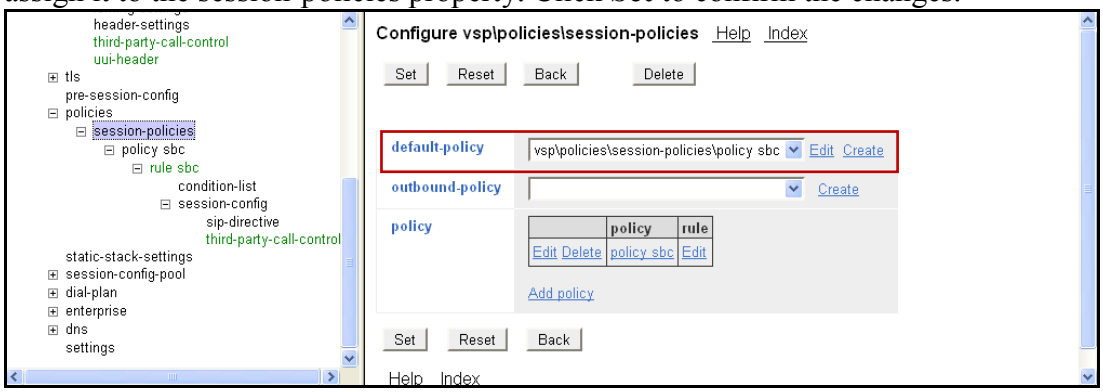


Create a Session Policy and Rule to Handle Perform Session Requests (continued)

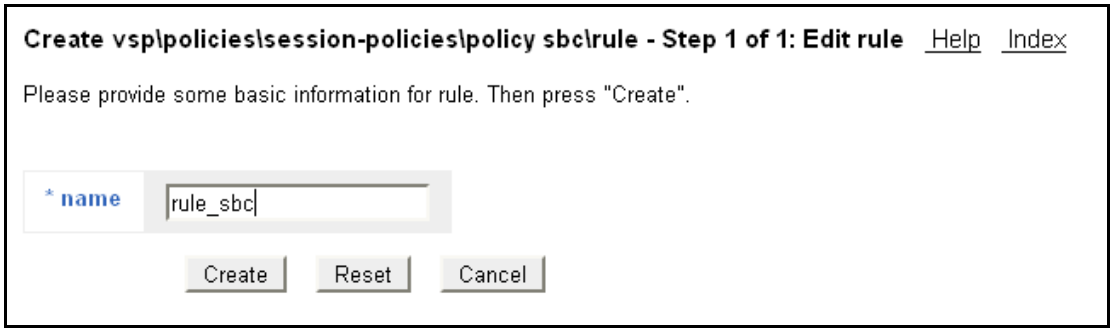
The **Add policy** link will prompt for a policy name, **policy_sbc** was used in the test. Click **Create** to create the policy.



Once the policy has been defined, select it from the **default-policy** selection box to assign it to the session-policies property. Click **Set** to confirm the changes.



Next, a rule must be created to instruct how to handle the Perform request. Click on the **Edit** link in the **Rule** column associated with the newly created policy. Assign a rule **name** and click **Create**.

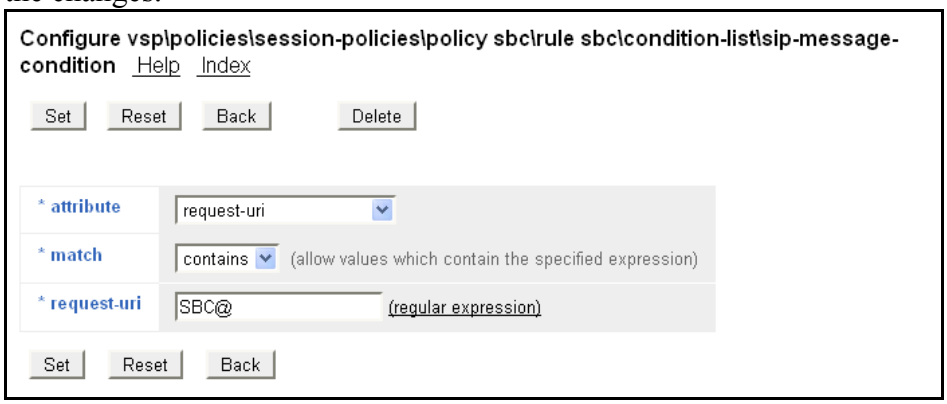


Create a Session Policy and Rule to Handle Perform Session Requests (continued)

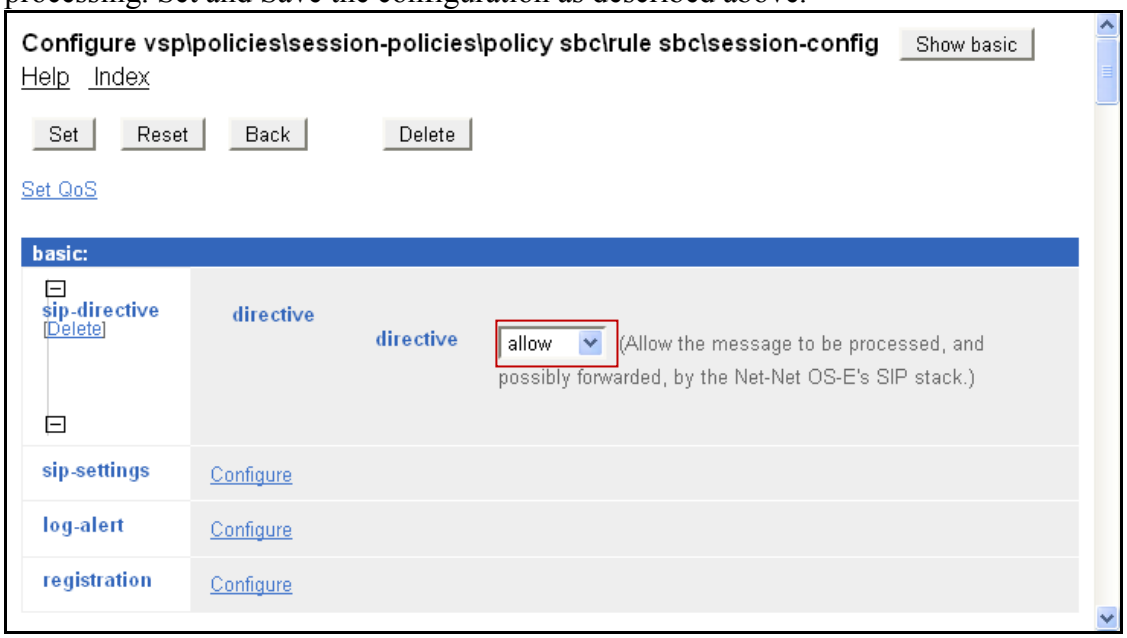
Click on the **rule_sbc** property in the navigation links (not shown) to configure the properties of the rule. In the test, **sbc** was the name given to the definition, **admin** was ***enabled***, and the **condition-list** object was expanded to define an ***AND*** **operation** to **evaluate** an attribute that would be contained in the request from Perform (see the next step for the attribute definition).

Create a Session Policy and Rule to Handle Perform Session Requests (continued)

Click on the **Edit** link associated with the **sip-message-condition** property to define the attributes of the condition. Select ***request-uri*** for the **attribute** option, ***contains*** for the **match** option, and enter **SBC@** for the **request-uri** value. Note, the request-uri value must match the Field Mapping entry made on the Perform server (SBC@10.64.22.112 was defined in the Perform configuration in **Section 9.1, Step 1**). Click **Set** to confirm the changes.

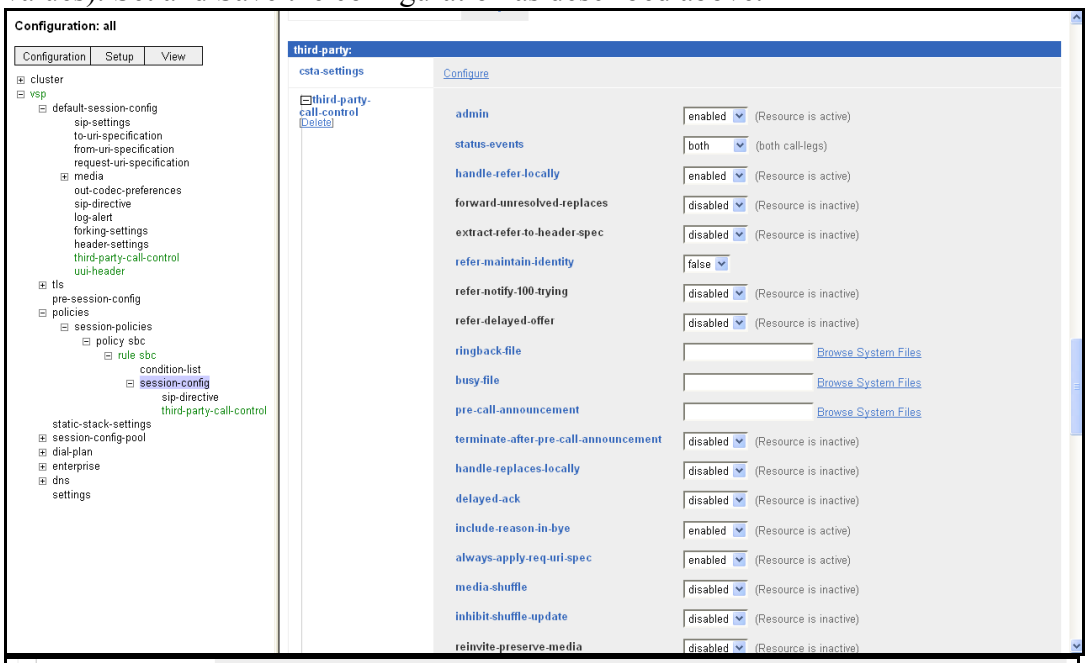


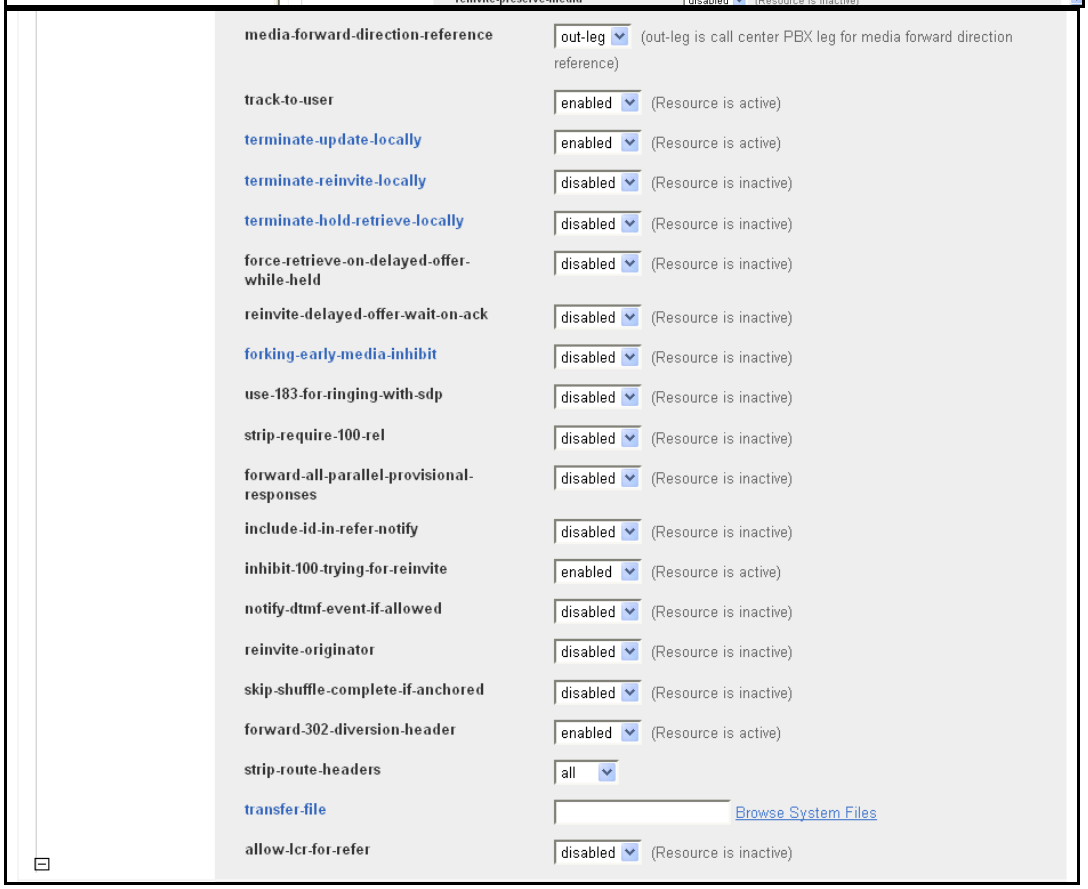
Next, select the **session-config** property in the navigation panel under the newly created **rule_sbc** property to enable additional properties for the policy. Scroll down to the **basic** settings, click on the + next to **sip-directive** to set the property to ***allow*** message processing. Set and Save the configuration as described above.



Create a Session Policy and Rule to Handle Perform Session Requests (continued)

Go to the third party heading and match the following settings (which should be default values): Set and Save the configuration as described above.



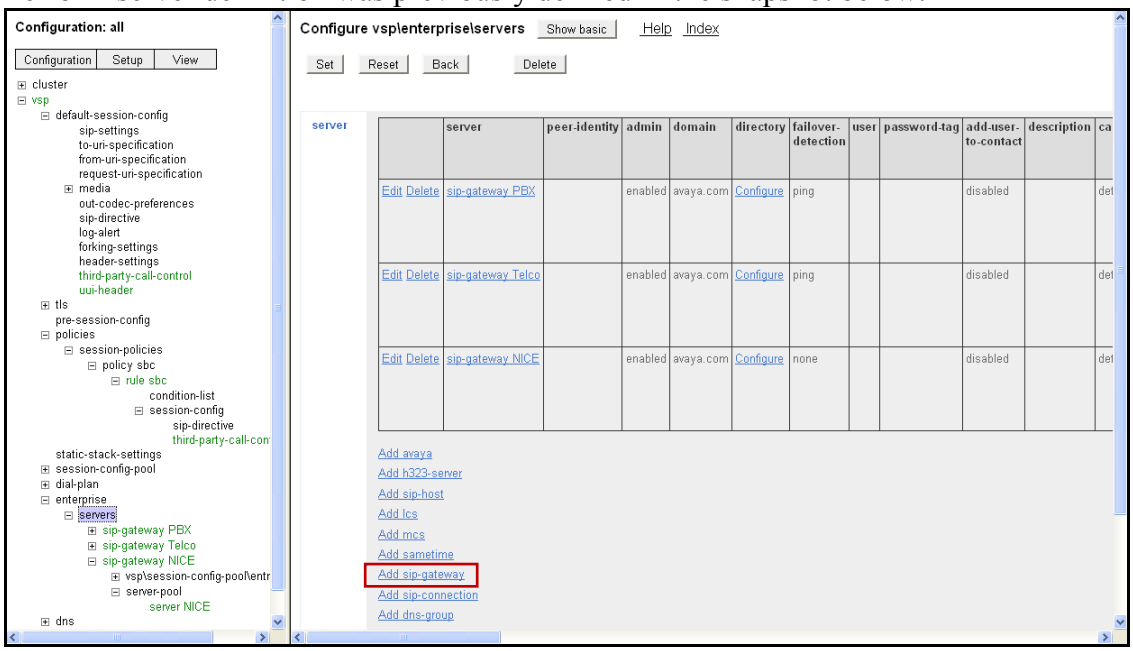


5. Create a SIP Gateway Server

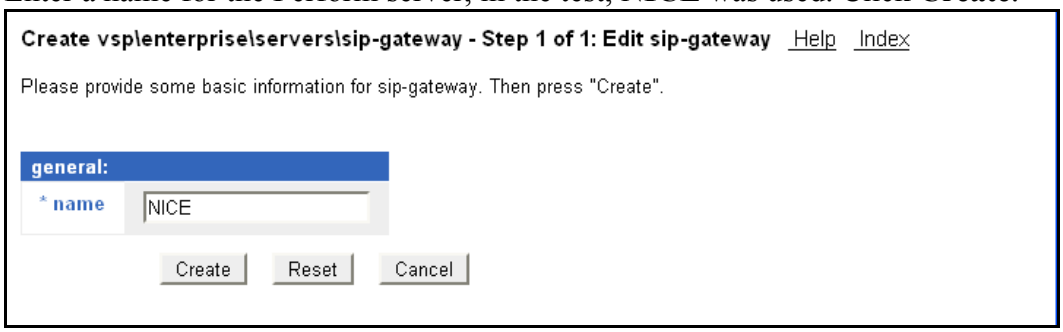
Note: This task requires several steps and spans the next three pages.

By default, the Perform server will appear to be an untrusted entity. By creating a definition for Perform as a SIP Gateway Server, the Session Border Controller will treat messages from this source as trusted and process the messages. Without this step, all requests from Perform would be ignored.

Navigate to the **vsp\enterprise\servers** property on the navigation panel, and select **Add sip-gateway** from the links below the existing PBX and Telco servers. Note that the Perform server definition was previously defined in the snapshot below.

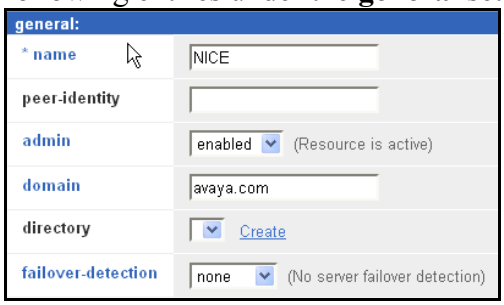


Enter a name for the Perform server, in the test, **NICE** was used. Click **Create**.

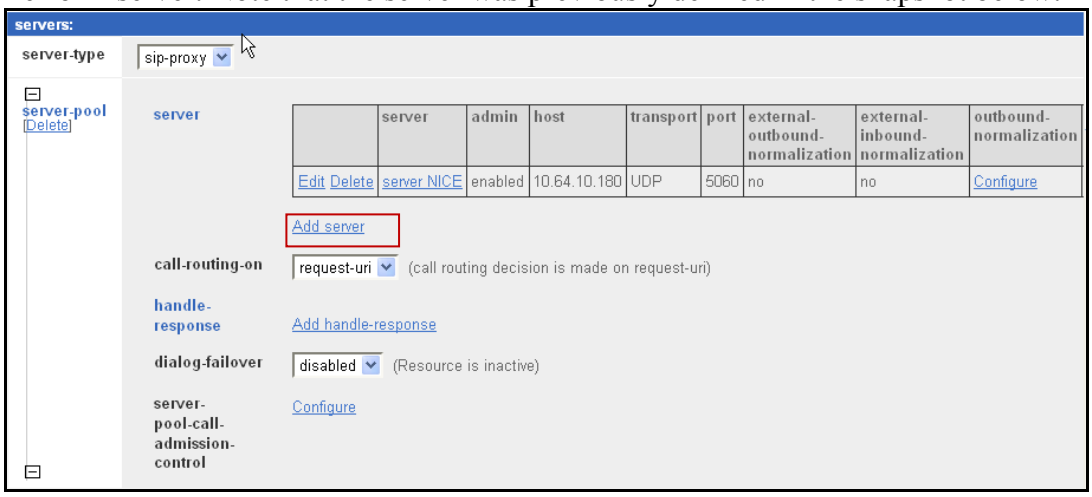


Create a NICE SIP Gateway Server (continued)

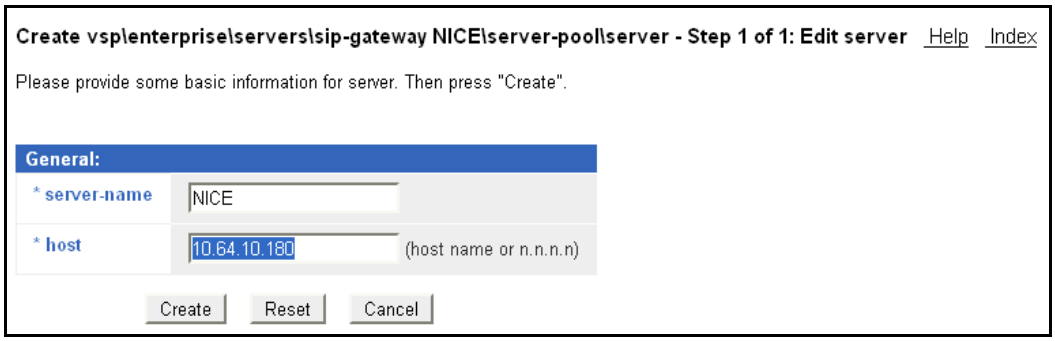
Select the newly created sip-gateway NICE object in the navigation pane, and make the following entries under the **general** settings:



In the **servers** section, select the **server-type: *sip-proxy*** and expand the **server-pool** object by selecting the + icon. Select the **Add server** link to define the details of the Perform server. Note that the server was previously defined in the snapshot below.

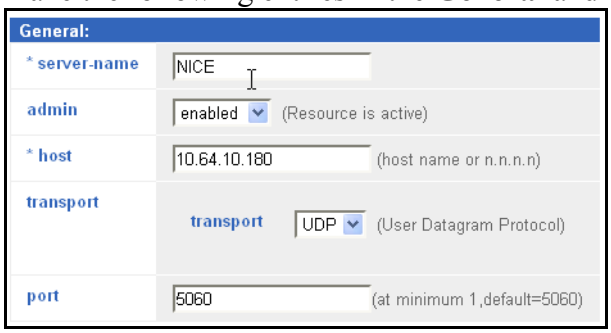


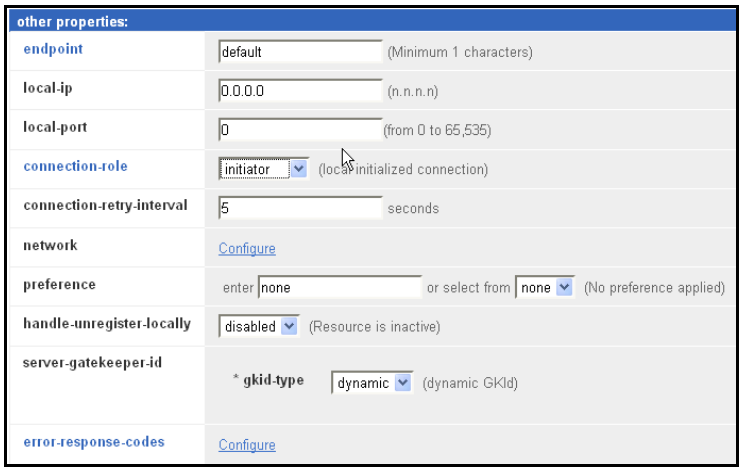
Enter the **host name** or **IP Address** and a **server-name.** Click **Create** which will return to the screen above.



Create a NICE SIP Gateway Server (continued)

Click the **Edit** link for the Perform server to add further details. Accept all defaults, and make the following entries in the **General** and **other properties** sections:





Set and Save the configuration as described above.

Note: the final configuration file was saved and can be reviewed here:

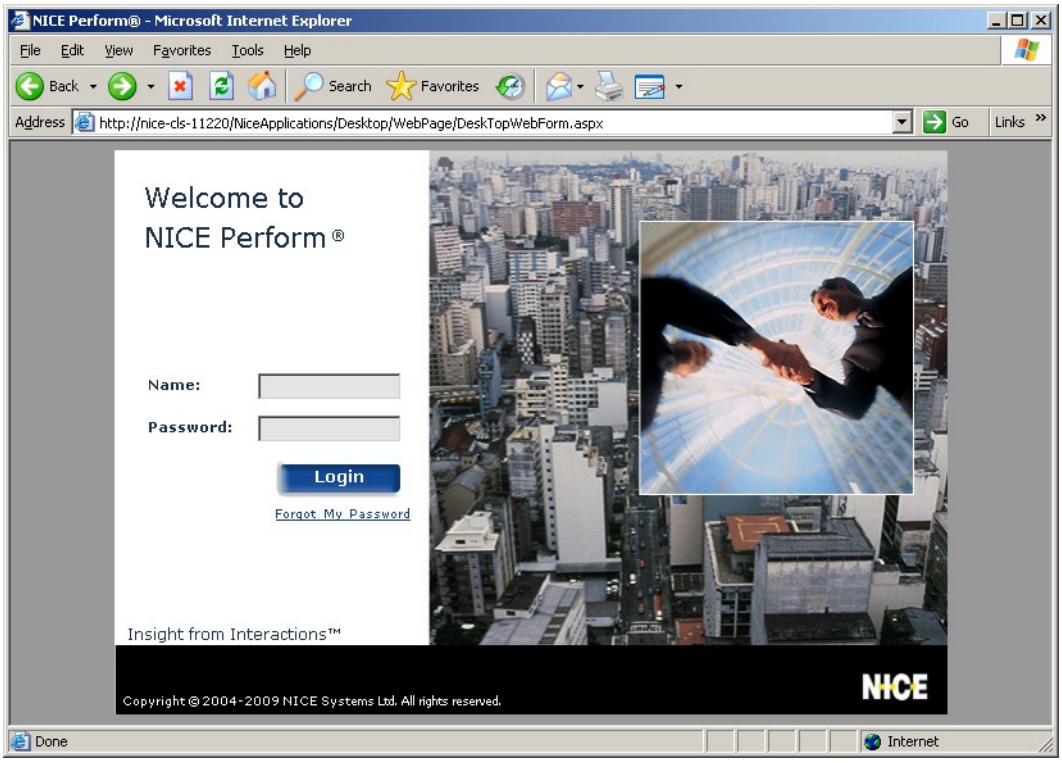
FinalSBC.cfg

9. Configure NICE Perform®

This section provides the steps for configuring the NICE Perform® solution.

9.1. NICE Perform Configuration Details

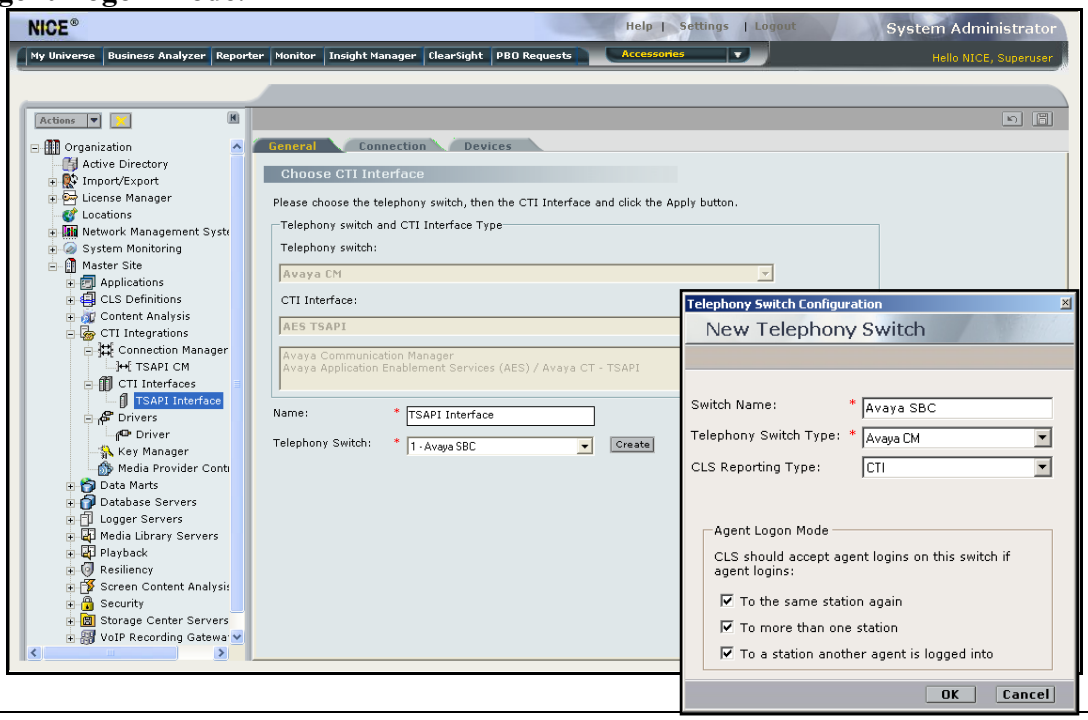
NICE Perform is configured using a web browser. Enter the URL of the Perform server such as http://<hostname>/nice where <hostname> is the ip address or fully qualified domain name of the Perform server. Login using appropriate credentials.

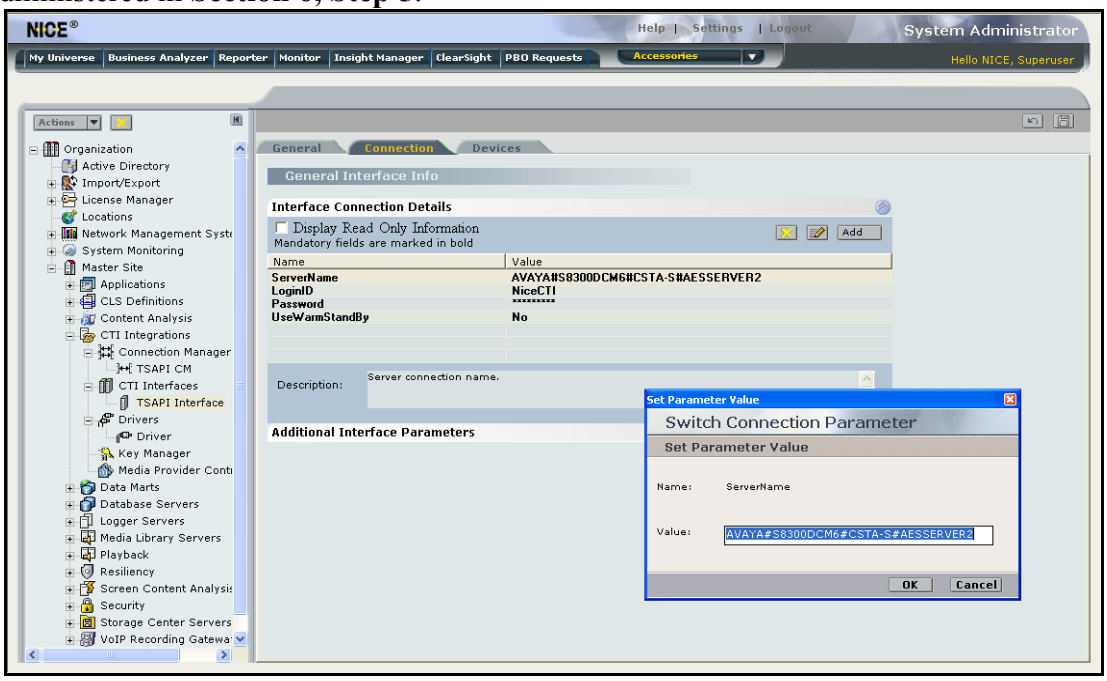


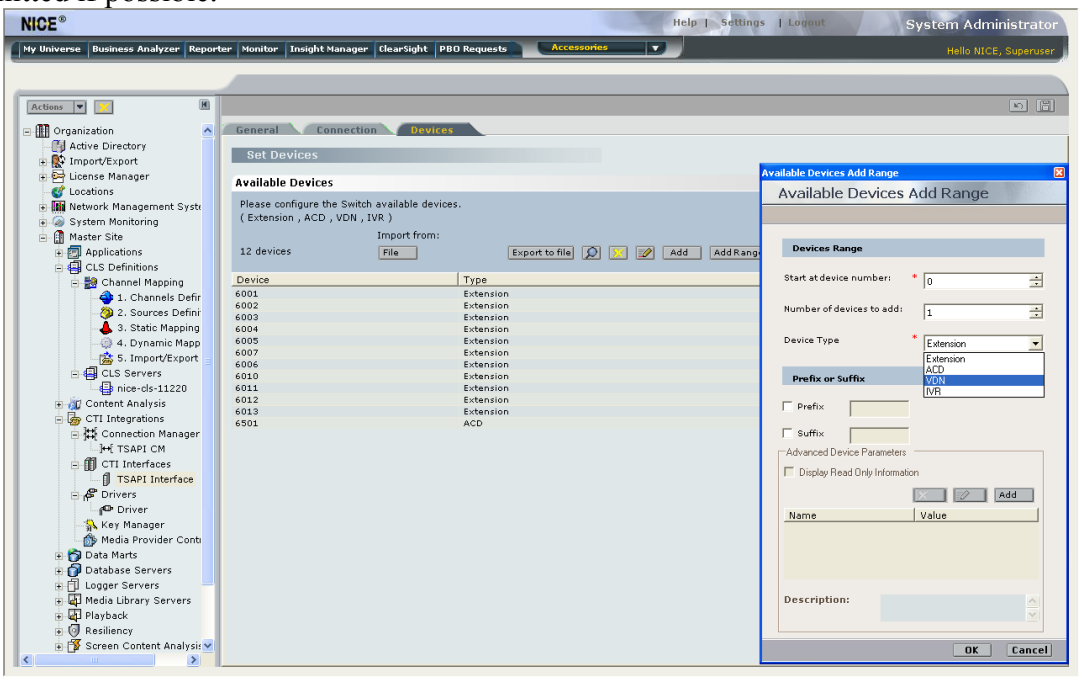
In general, the steps were as follows:

- Configure the Application Enablement Services Interface
- Configure the Logger Channel Mappings

Note that each of these steps requires several subtasks, the illustrations of these subtasks cover several pages to complete each task.

Step	Description
1.	**Configure the Application Enablement Services Interface** Users with System Administration privileges will have the option to select **System Administrator** from the **Accessories** menu. Navigation involves clicking on the objects in the navigation tree on the left panel of the browser window. Navigate to the **Master Site > CTI Integrations > CTI Interfaces > TSAPI Interface** object in the navigation tree and enter a **Name** for the CTI Interface (***TSAPI Interface*** was used in the test. Click **Create** to define the **Telephony Switch,** ***Avaya SBC*** was entered for the **Switch Name**, and ***Avaya CM*** was used for the **Telephony Switch Type**. The **CLS Reporting Type *CTI*** was selected and defaults were used for the **Agent Logon Mode**. 

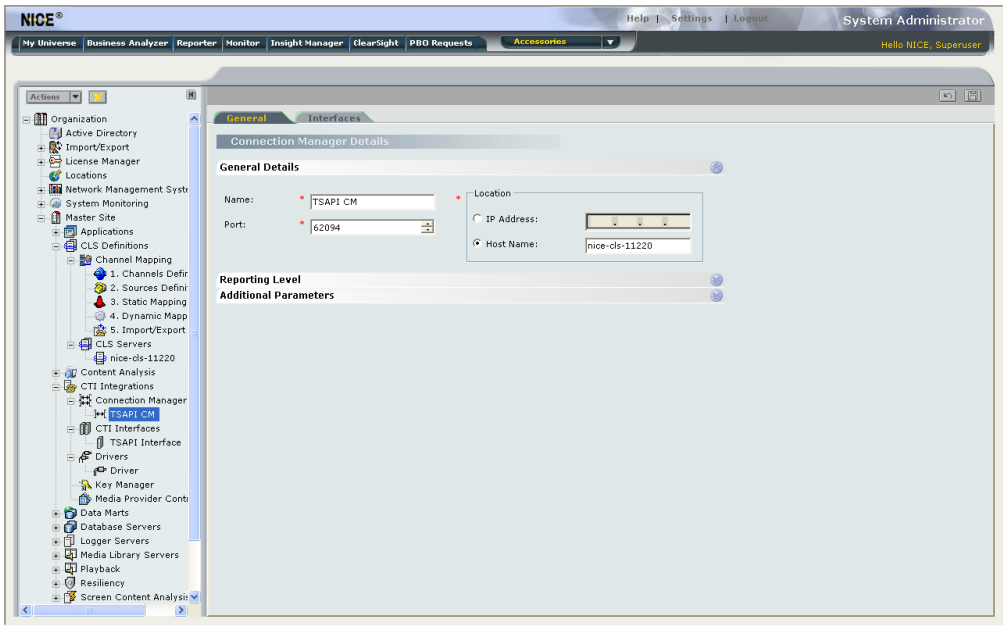
Step	Description
	Configure the Application Enablement Services Interface (continued) Click on the **Connection** tab and click the **Edit** icon for each parameter in the **Interface Connection Details** section. Enter the TLINK name from **Section 6, Step 7** above for the **ServerName** parameter. Similarly, enter the **LoginID** and **Password** as administered in **Section 6, Step 5**. 

Step	Description
	Configure the Application Enablement Services Interface (continued) On the **Devices** Tab, create an entry for each Extension, ACD (lead Hunt Group Extension), and VDN that the application will need to monitor in Communication Manager for CTI events. Entry can be simplified if the devices are in a continuous range by using the Devices Range entries, however caution should be excersised with this approach as each invalid device in the range will generate warnings and should be omitted if possible. 

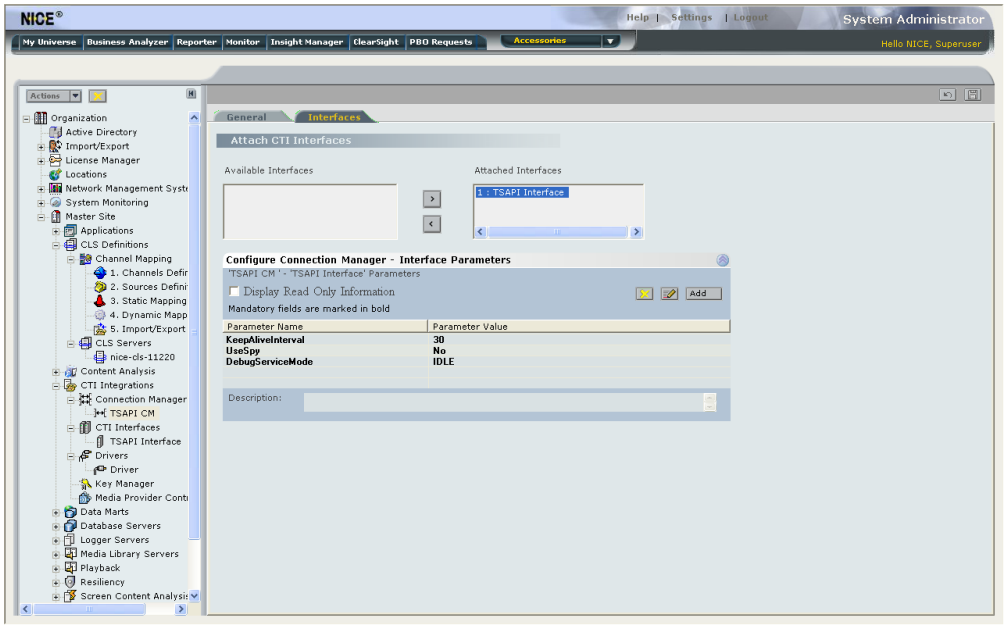
Configure the Application Enablement Services Interface (continued)

The Connection Manager defines how internal modules of the Perform solution will communicate with the CTI Interface module.

Navigate to the **Master Site > CTI Integrations >Connection Manager > TSAPI CM** object in the navigation tree and enter the **Name** and **Port** to use for the connection under the **General Details** section, and enter the **Host Name** of the Perform server in the **Location** section.

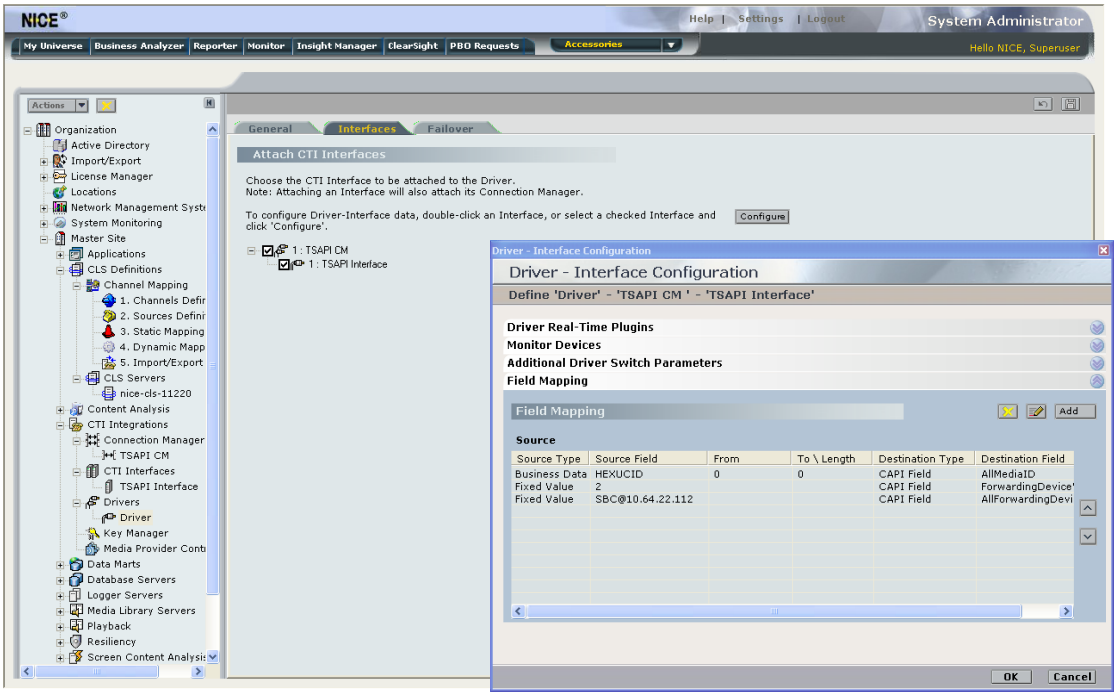


On the **Interfaces** tab, highlight the ***TSAPI Interface*** in the **Available Interfaces** column and use the **>** button to move this interface into the **Attached Interfaces** column. All other settings were defaults.

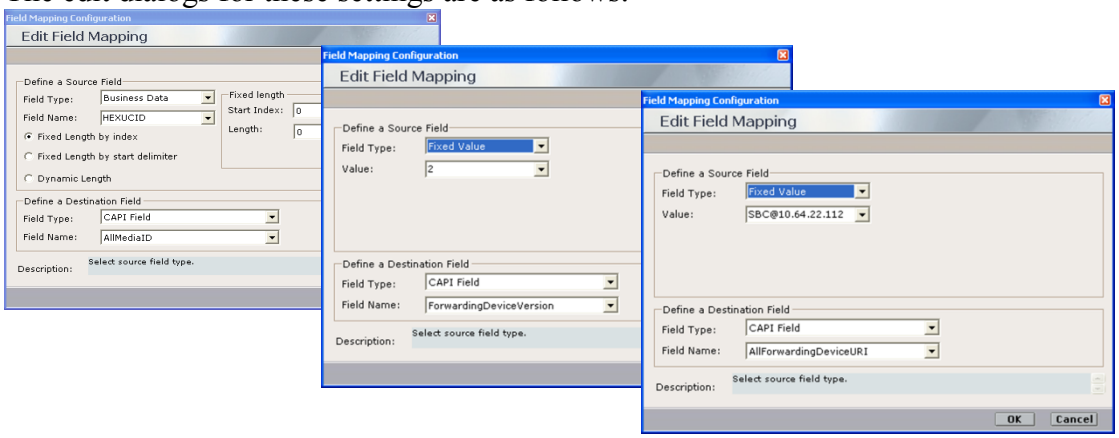


Configure the Application Enablement Services Interface (continued)

Next, navigate to the **Master Site > CTI Integrations > Drivers > Driver** object to link the ***TSAPI Interface***. Click on the **Configure** button to define additional settings in the **Field Mapping** section. These settings are entered using the **Edit** button. The **Business Data (*HEXUCID)***, and **Fixed Value** (*SBC@10.64.22.112)* are settings the driver will use to send SIP Invites to the Session Border Controller.

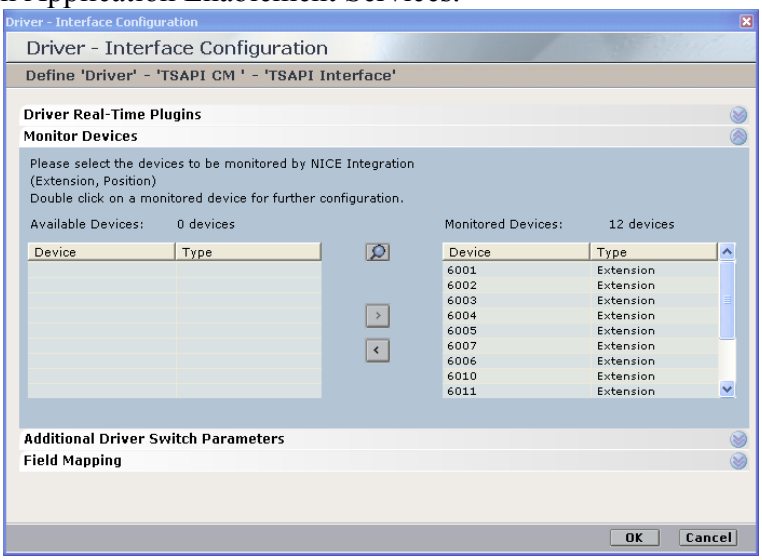


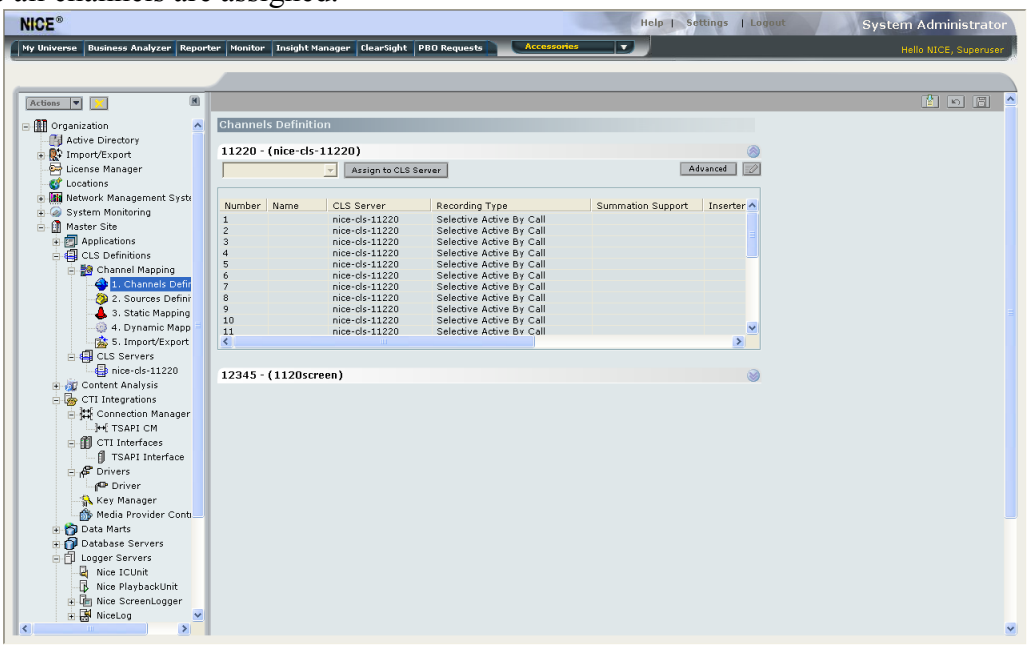
The edit dialogs for these settings are as follows:



Configure the Application Enablement Services Interface (continued)

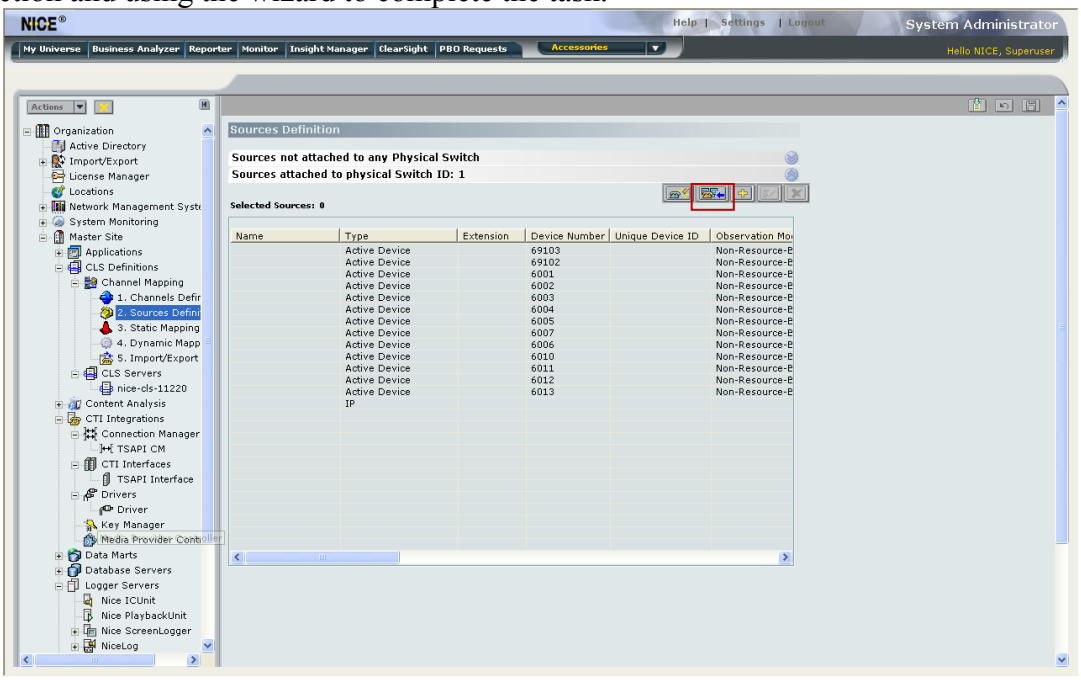
In addition, open the **Monitor Devices** section and move all of the **Available Devices** into the **Monitored Devices** column using the **>** button. This is the last step in configuring the devices the driver will use to request TSAPI Monitors when it starts a connection with Application Enablement Services.



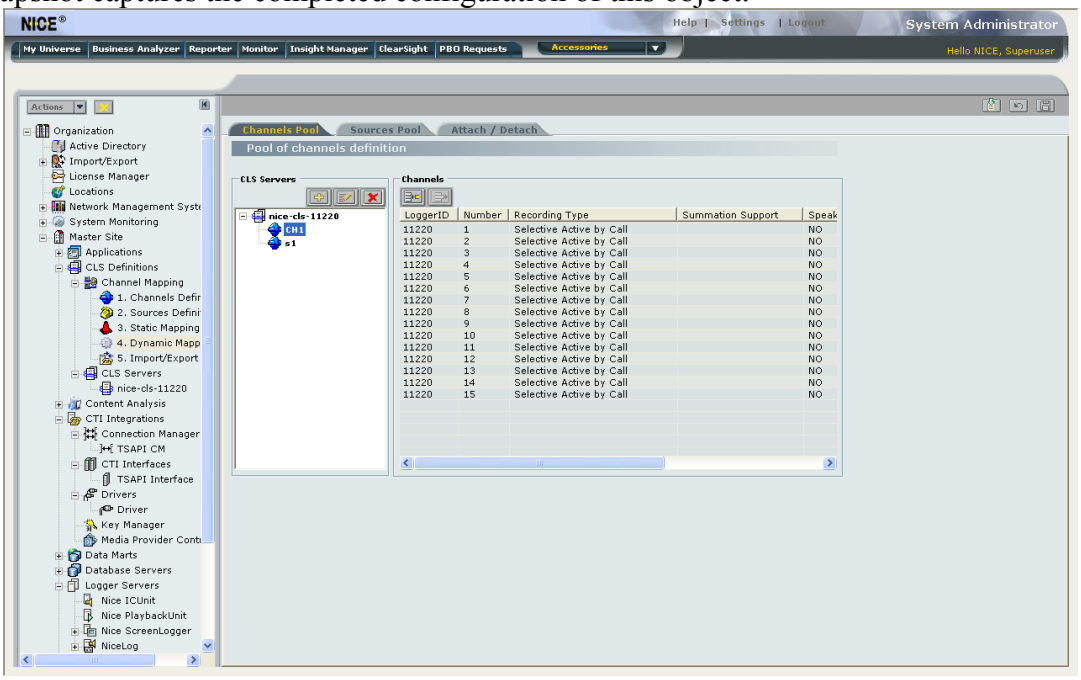
2.	**Configure the Logger Channel Mappings** The Logger is the module that will be responsible for dedicating an available "channel" for each call to be recorded, initiating the Invite to the Session Border Controller, and receiving and storing the RTP media sent from the Session Border Controller. Navigate to the **Master Site > CLS Definitions > Channel Mapping > Channels Definition** object in the navigation tree. For each channel, click the **Edit** button and set the **Recording Type** to ***Selective Active By Call***. The dialog looks similar to those above, but is not available to illustrate as the system blocks modifying the configuration once all channels are assigned. 

Configure the Logger Channel Mappings (continued)

In **Sources Definition** create your sources as ***Active Device*** using the **Import Sources from CTI Interface** button  under the **Sources attached to physical Switch ID: 1** section and using the wizard to complete the task.

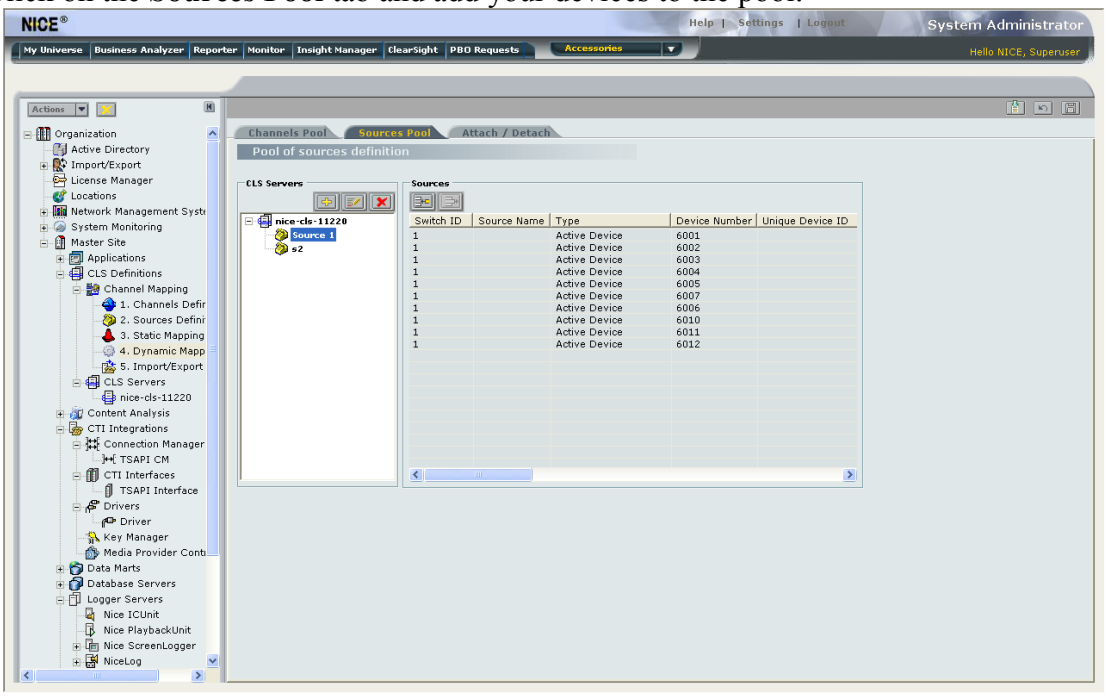


Next, go to **Dynamic Mapping** and define a new channel pool using the  button. This snapshot captures the completed configuration of this object.

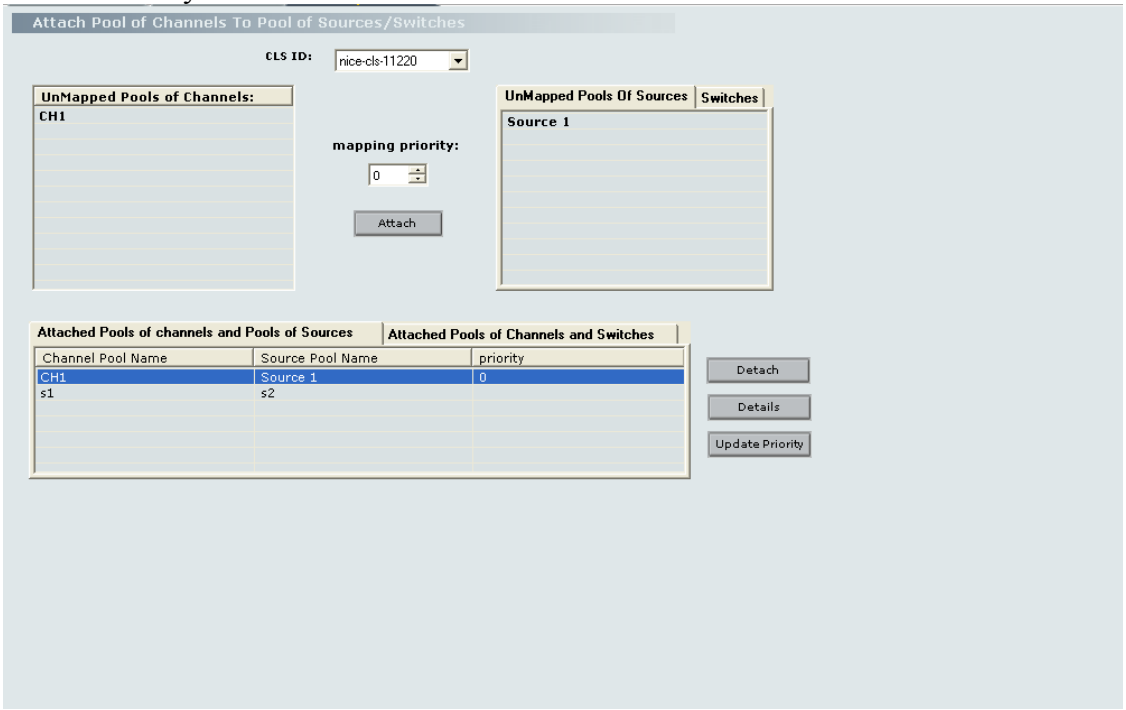


Configure the Logger Channel Mappings (continued)

Click on the **Sources Pool** tab and add your devices to the pool:

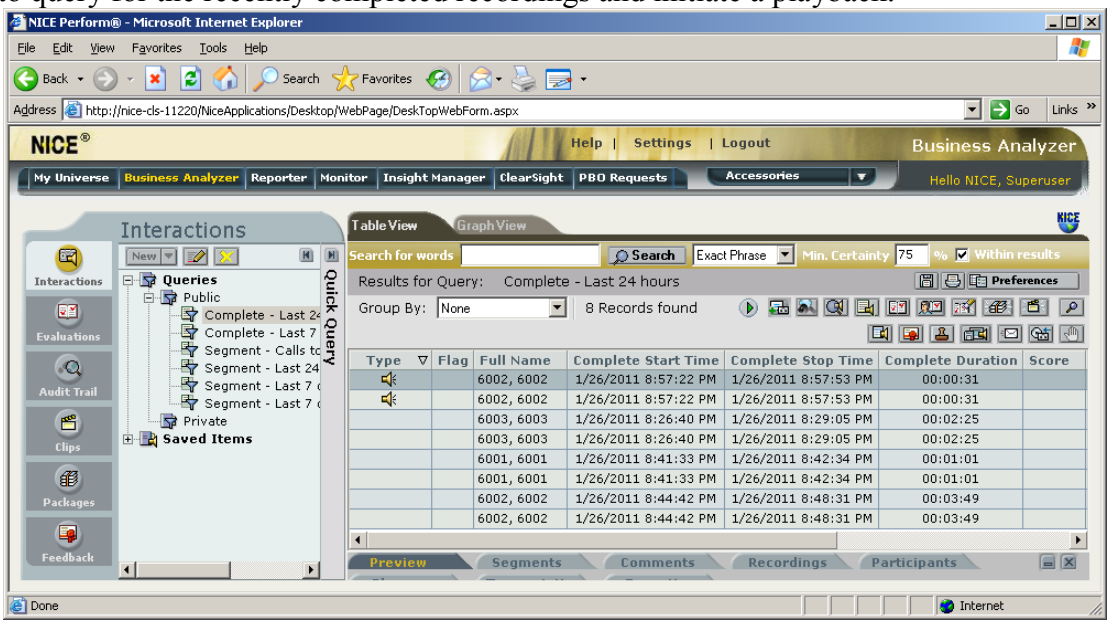


Finally Go to the **Attach /Detach** tab and attach the pool of channels to the pool of sources. When complete, click Save and Update Configuration buttons on the top right corner of the System Administrator interface.

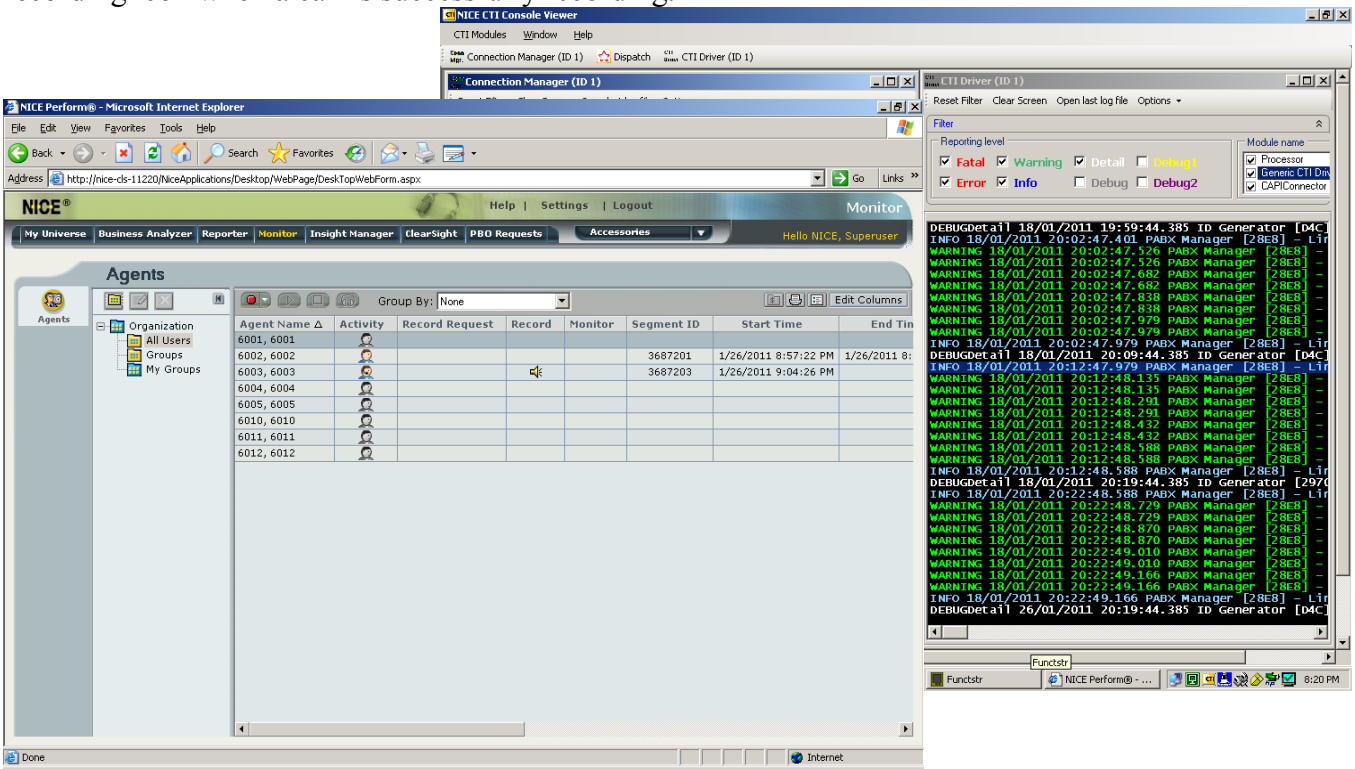


10. Verification Steps

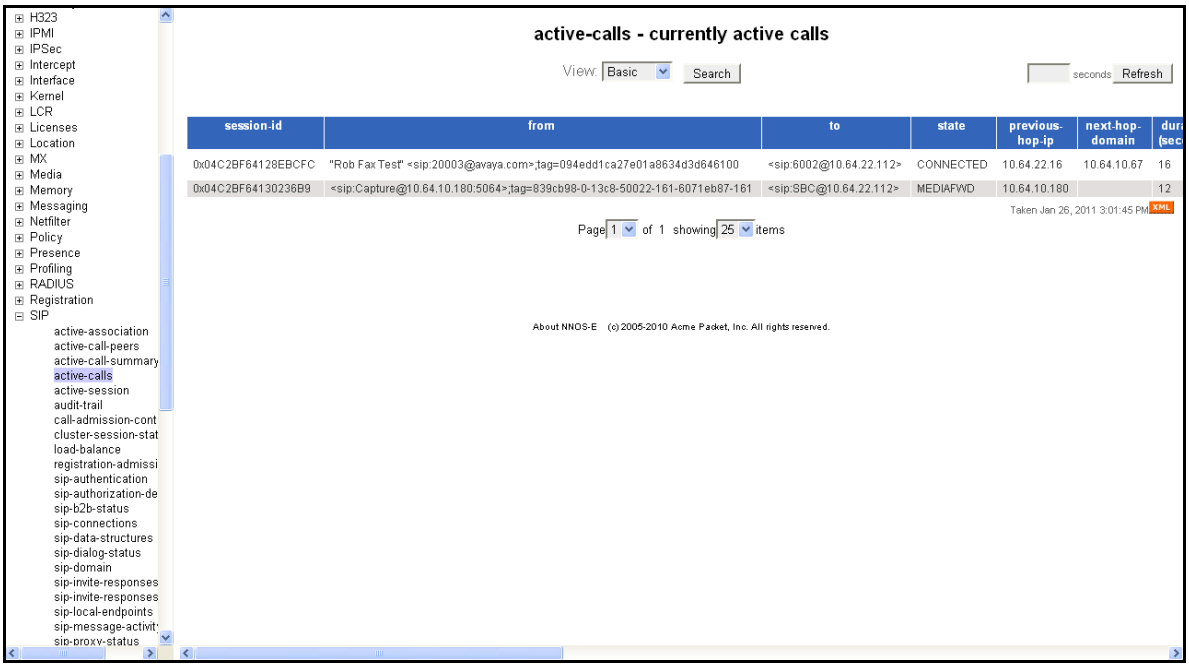
Following each completed test case, the NICE Perform Business Analyzer user application was used to query for the recently completed recordings and initiate a playback.



In addition, the Console Viewer application shown below displays the status of CTI Driver and inter-process communications on the Nice Perform server. The Monitor application will display a recording icon when a call is successfully recording.



On the Session Border Controller, the Status tab enables a view of active SIP calls, when the Perform application is successfully recording a call, a MEDIAFWD session will appear in the active call status screen:



11. Conclusion

Nice Perform® successfully demonstrated the ability to record calls that passed through the Avaya Aura® Session Border Controller. Further, the application demonstrated the ability to successfully recover from network and server outages with minimal delay in recovering to full functionality.

12. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com.

Administering Avaya Aura™ SessionManager, Document ID 03-603324, Issue 1, Release 6.1, November, 2010.
Avaya Aura™ Application Enablement Services Administration and Maintenance Guide, Document ID 02-300357, Issue 11, Release 5.2, November, 2009.
Avaya Aura™ SBC System Administration Guide, V6.0
Avaya Aura™ SBC Objects and Properties Reference, V6.0
Administering Avaya Aura™ Communication Manager Server Options, Document ID 03-603479, Issue 2, Release 6.0, June, 2010.
Administering Avaya Aura™ Communication Manager, Document ID 03-300509, Issue 6.0, Release 6.0, June, 2010.

Product information for Nice Perform® may be found in help screens on the Nice Perform® application server and online at http://www.nice.com

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.